S03P0945US00

日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　８月　１日

出願番号
Application Number: 特願２００２－２２５２７７

[ST.10/C]: [ＪＰ２００２－２２５２７７]

出願人
Applicant(s): ソニー株式会社

２００３年　５月２７日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０３９２９１

【書類名】　特許願
【整理番号】　0290442405
【提出日】　平成14年 8月 1日
【あて先】　特許庁長官　及川　耕造　殿
【国際特許分類】　G06F 17/30
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号ソニー株式会社内
　【氏名】　荻野　晃
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100082740
　【弁理士】
　【氏名又は名称】　田辺　恵基
【手数料の表示】
　【予納台帳番号】　048253
　【納付金額】　21,000円
【提出物件の目録】
　【物件名】　明細書　1
　【物件名】　図面　1
　【物件名】　要約書　1
　【包括委任状番号】　9709125
【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　コンテンツ配信システム及びコンテンツ配信方法並びに端末装置

【特許請求の範囲】

【請求項１】

配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信システムにおいて、

上記配信サーバでは、

上記端末装置に割り当てられた固有のユーザ識別情報と、上記端末装置側で予め状態が設定された格納定義フラグとを所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報を上記コンテンツに重畳する重畳手段と、

上記透かし情報が重畳されたコンテンツに所定の暗号をかける暗号化手段と、

上記暗号がかけられたコンテンツを上記ネットワークを介して上記端末装置に送信する送信手段と

を具え、

上記端末装置では、

上記コンテンツを受信する受信手段と、

上記コンテンツに重畳されている上記透かし情報を所定の処理を行うようにして上記ユーザ識別情報及び上記格納定義フラグを抽出する抽出手段と、

上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、上記コンテンツにかけられている上記暗号を解除する暗号解除手段と、

上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、上記暗号が解除されたコンテンツを格納するか否かを判断する判断手段と、

上記判断手段の判断結果に応じて、上記透かし情報が重畳されているコンテンツを格納する格納手段と

を具えることを特徴とするコンテンツ配信システム。

【請求項２】

上記ネットワーク上に設けられ、上記端末装置から発信されるコンテンツを監視しながら、当該コンテンツから上記ユーザ識別情報が検出された場合には、当

該端末装置に所定の通知又は警告を発信する監視サーバ

を具えることを特徴とする請求項１に記載のコンテンツ配信システム。

【請求項３】

上記監視サーバは、

検出した上記ユーザ識別情報が上記端末装置に割り当てられた固有のユーザ識別情報と一致するか否かに応じて当該端末装置に上記通知又は上記警告を発信する

ことを特徴とする請求項２に記載のコンテンツ配信システム。

【請求項４】

配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、

上記配信サーバでは、

上記端末装置に割り当てられた固有のユーザ識別情報と、上記端末装置側で予め状態が設定された格納定義フラグとを所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報を上記コンテンツに重畳する第１のステップと、

上記透かし情報が重畳されたコンテンツに所定の暗号をかける第２のステップと、

上記暗号がかけられたコンテンツを上記ネットワークを介して上記端末装置に送信する第３のステップと

を具え、

上記端末装置では、

上記コンテンツを受信する第４のステップと、

上記コンテンツに重畳されている上記透かし情報を所定の処理を行うようにして上記ユーザ識別情報及び上記格納定義フラグを抽出する第５のステップと、

上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、上記コンテンツにかけられている上記暗号を解除する第６のステップと、

上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、上記暗号が解除されたコンテンツを格納するか否かを判断する第７のステップと

上記判断結果に応じて、上記透かし情報が重畳されているコンテンツを格納する第８のステップと

を具えることを特徴とするコンテンツ配信方法。

【請求項５】

上記ネットワーク上で上記端末装置から発信されるコンテンツを監視しながら、当該コンテンツから上記ユーザ識別情報が検出された場合には、当該端末装置に所定の通知又は警告を発信する第９のステップ

を具えることを特徴とする請求項４に記載のコンテンツ配信方法。

【請求項６】

上記第９のステップでは、

検出した上記ユーザ識別情報が上記端末装置に割り当てられた固有のユーザ識別情報と一致するか否かに応じて当該端末装置に上記通知又は上記警告を発信する

ことを特徴とする請求項５に記載のコンテンツ配信方法。

【請求項７】

配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、

上記配信サーバでは、

上記端末装置に割り当てられた固有のユーザ識別情報と、上記端末装置側で予め状態が設定された格納定義フラグとを上記コンテンツに付加する第１のステップと、

上記ユーザ識別情報及び上記格納定義フラグが付加されたコンテンツに所定の暗号をかける第２のステップと、

上記暗号がかけられたコンテンツを上記ネットワークを介して上記端末装置に送信する第３のステップと

を具え、

上記端末装置では、

上記コンテンツを受信する第４のステップと、

上記コンテンツに付加されている上記ユーザ識別情報及び上記格納定義フラグを抽出する第５のステップと、

上記格納定義フラグの状態に応じて上記コンテンツにかけられている上記暗号を解除する第６のステップと、

上記ユーザ識別情報の有効性に基づいて当該ユーザ識別情報を所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報を上記コンテンツに重畳するか否かを判断する第７のステップと、

上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、上記暗号が解除された上記コンテンツを格納するか否かを判断する第８のステップと、

上記判断結果に応じて上記透かし情報が重畳されたコンテンツを格納する第９のステップと

を具えることを特徴とするコンテンツ配信方法。

【請求項８】

配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、

上記配信サーバでは、

上記端末装置に割り当てられた固有のユーザ識別情報と、上記端末装置側で予め状態が設定された格納定義フラグとを上記コンテンツに付加する第１のステップと、

上記ユーザ識別情報及び上記格納定義フラグが付加されたコンテンツに所定の暗号をかける第２のステップと、

上記暗号がかけられたコンテンツを上記ネットワークを介して上記端末装置に送信する第３のステップと

を具え、

上記端末装置では、

上記コンテンツを受信して所定の格納手段に格納する第４のステップと、

上記格納手段から必要に応じて上記コンテンツを再生した場合、当該コンテンツに付加されている上記ユーザ識別情報及び上記格納定義フラグを抽出する第５

のステップと、

上記格納定義フラグの状態に応じて上記コンテンツにかけられている上記暗号を解除する第６のステップと、

上記ユーザ識別情報を所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報を上記暗号が解除された上記コンテンツに重畳する第７のステップと、

上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、上記透かし情報が重畳されたコンテンツを上記格納手段に格納するか否かを判断する第８のステップと、

上記判断結果に応じて上記透かし情報が重畳されたコンテンツを上記格納手段に格納する第９のステップと

を具えることを特徴とするコンテンツ配信方法。

【請求項９】

コンテンツを管理する端末装置において、

上記コンテンツに、上記端末装置に割り当てられた固有のユーザ識別情報と、上記端末装置側で予め状態が設定された格納定義フラグとが所定の拡散変調により変換された透かし情報として重畳されている場合、当該コンテンツに重畳されている上記透かし情報を所定の処理を行うようにして上記ユーザ識別情報及び上記格納定義フラグを抽出する抽出手段と、

上記コンテンツに暗号がかけられている場合、上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、当該コンテンツにかけられている上記暗号を解除する暗号解除手段と、

上記ユーザ識別情報の有効性及び又は上記格納定義フラグの状態に基づいて、上記暗号が解除されたコンテンツを格納するか否かを判断する判断手段と、

上記判断手段の判断結果に応じて、上記透かし情報が重畳されているコンテンツを格納する格納手段と

を具えることを特徴とする端末装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はコンテンツ配信システム及びコンテンツ配信方法並びに端末装置に関し、例えばインターネット等を用いたコンテンツ配信システムに適用して好適なものである。

【０００２】

【従来の技術】

従来、この種のコンテンツ配信システムでは、配信側のサーバが、インターネット等のネットワークを介して接続された複数の個人端末のうちユーザからの要求等のあった個人端末に対して、文章、画像及び音声等の素材データを種々のシナリオで編集したデータ群（以下、これをコンテンツと呼ぶ）を配信するようになされている。

【０００３】

その際、配信側のサーバは、該当するコンテンツを送信前に所定の暗号で暗号化する一方、ネットワークを介してコンテンツを受信したユーザ側の個人端末は、当該コンテンツにかけられた暗号を解除した場合のみ視聴することができるようになされた暗号化処理方式を採用するのが一般的である。

【０００４】

【発明が解決しようとする課題】

ところが、かかる暗号化処理方式を採用したコンテンツ配信システムでは、ユーザによる最終的な視聴は暗号を解除した後でしか行い得ないため、個人端末におけるハードディスクや外部メモリ等に格納されているコンテンツが外部に取り出された場合には、当該コンテンツが不正に複製され、又はネットワーク上に流出された場合でも、そのようなリーケージパスを防ぐことは非常に困難であった。

【０００５】

仮にこのような不正に複製され又はネットワーク上に流出されたコンテンツを発見した場合でも、当該コンテンツを不正に取得した者を特定することや、発見したコンテンツの同一性の確認を行うことが困難であることから、法的規制以外で不正流通の防止手段を講じる必要があった。

【０００６】

そしてこのようなディジタルコピーが容易に行われてしまうと、オリジナルのコンテンツと全く同じコピーができてしまうため、著作権保護を強化せざるを得ない状況となる。その結果、従来より一層、ユーザへの利用制限が厳しくなってしまい、正規にコンテンツを購入したユーザからは不満の声が上がる一方となるおそれがあった。

【０００７】

本発明は以上の点を考慮してなされたもので、正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信システム及びコンテンツ配信方法並びに端末装置を提案しようとするものである。

【０００８】

【課題を解決するための手段】

かかる課題を解決するため本発明においては、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信システムにおいて、配信サーバでは、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとを所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報をコンテンツに重畳する重畳手段と、透かし情報が重畳されたコンテンツに所定の暗号をかける暗号化手段と、暗号がかけられたコンテンツをネットワークを介して端末装置に送信する送信手段とを設け、端末装置では、コンテンツを受信する受信手段と、コンテンツに重畳されている透かし情報を所定の処理を行うようにしてユーザ識別情報及び格納定義フラグを抽出する抽出手段と、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、コンテンツにかけられている暗号を解除する暗号解除手段と、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する判断手段と、判断手段の判断結果に応じて、透かし情報が重畳されているコンテンツを格納する格納手段とを設けるようにした。

【０００９】

この結果このコンテンツ配信システムでは、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随する

こととなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができる。

【００１０】

また本発明においては、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、配信サーバでは、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとを所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報をコンテンツに重畳する第１のステップと、透かし情報が重畳されたコンテンツに所定の暗号をかける第２のステップと、暗号がかけられたコンテンツをネットワークを介して端末装置に送信する第３のステップとを設け、端末装置では、コンテンツを受信する第４のステップと、コンテンツに重畳されている透かし情報を所定の処理を行うようにしてユーザ識別情報及び格納定義フラグを抽出する第５のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、コンテンツにかけられている暗号を解除する第６のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する第７のステップと、判断結果に応じて、透かし情報が重畳されているコンテンツを格納する第８のステップとを設けるようにした。

【００１１】

この結果このコンテンツ配信方法では、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができる。

【００１２】

さらに本発明においては、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、配信サーバでは、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとをコンテンツに付加する第１のステップと、ユーザ識別情報及び格納定義フラグが付加されたコンテンツに所定の暗号をかける第２のステップと、暗号がか

けられたコンテンツをネットワークを介して端末装置に送信する第３のステップとを設け、端末装置では、コンテンツを受信する第４のステップと、コンテンツに付加されているユーザ識別情報及び格納定義フラグを抽出する第５のステップと、格納定義フラグの状態に応じてコンテンツにかけられている暗号を解除する第６のステップと、ユーザ識別情報の有効性に基づいて当該ユーザ識別情報を所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報をコンテンツに重畳するか否かを判断する第７のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する第８のステップと、判断結果に応じて透かし情報が重畳されたコンテンツを格納する第９のステップとを設けるようにした。

【００１３】

この結果このコンテンツ配信方法では、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができる。

【００１４】

さらに本発明においては、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、配信サーバでは、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとをコンテンツに付加する第１のステップと、ユーザ識別情報及び格納定義フラグが付加されたコンテンツに所定の暗号をかける第２のステップと、暗号がかけられたコンテンツをネットワークを介して端末装置に送信する第３のステップとを設け、端末装置では、コンテンツを受信して所定の格納手段に格納する第４のステップと、格納手段から必要に応じてコンテンツを再生した場合、当該コンテンツに付加されているユーザ識別情報及び格納定義フラグを抽出する第５のステップと、格納定義フラグの状態に応じてコンテンツにかけられている暗号を解除する第６のステップと、ユーザ識別情報を所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報を暗号が解除されたコンテンツに重畳する第７のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に

基づいて、透かし情報が重畳されたコンテンツを格納手段に格納するか否かを判断する第８のステップと、判断結果に応じて透かし情報が重畳されたコンテンツを格納手段に格納する第９のステップとを設けるようにした。

【００１５】

この結果このコンテンツ配信方法では、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができる。

【００１６】

さらに本発明においては、コンテンツを管理する端末装置において、コンテンツに、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとが所定の拡散変調により変換された透かし情報として重畳されている場合、当該コンテンツに重畳されている透かし情報を所定の処理を行うようにしてユーザ識別情報及び格納定義フラグを抽出する抽出手段と、コンテンツに暗号がかけられている場合、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、当該コンテンツにかけられている暗号を解除する暗号解除手段と、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する判断手段と、判断手段の判断結果に応じて、透かし情報が重畳されているコンテンツを格納する格納手段とを設けるようにした。

【００１７】

この結果この端末装置では、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができる。

【００１８】

【発明の実施の形態】

以下図面について、本発明の一実施の形態を詳述する。

【００１９】

（１）第１の実施の形態

（１－１）第１の実施の形態によるコンテンツ配信システムの全体構成

図１において、１は全体として本実施の形態によるコンテンツ配信システムを示し、ユーザが使用する複数の個人端末２（2_1～2_n）と、サービス提供業者側が配置した配信サーバ３及び監視サーバ４とがネットワーク５を介して接続されることにより構成されている。

【００２０】

各個人端末２においては、一般家庭や会社内に設置された通常のパーソナルコンピュータであり、他の個人端末２や配信サーバ３とネットワーク５を介して通信することにより必要なデータを送受信したり、当該通信により得られた画面データに基づくＷｅｂページ画面等をディスプレイ表示することができるようになされている。

【００２１】

また配信サーバ３は、サービス提供業者側が提供する後述のような各種サービスに関する各種処理を行うＷｅｂサーバ及びデータベースサーバであり、ネットワーク５を介してアクセスしてきた個人端末２と通信して必要なコンテンツを送受信することができるようになされている。

【００２２】

さらに監視サーバ４は、サービス提供業者側が各個人端末２から発信されるコンテンツのうち著作権侵害に該当するコンテンツの有無をネットワーク上を常時巡回しながら監視し、著作権侵害に該当するコンテンツを検出した場合には、当該コンテンツを発信した個人端末に対して所定の警告をネットワークを介して通知することができるようになされている。

【００２３】

（１－２）配信サーバの具体的構成

ここで配信サーバ３の構成を図２に示す。この図２からも明らかなように、配信サーバ３は、配信サーバ３全体の制御を司るＣＰＵ（Central Processing Unit）１０と、各種ソフトウェアが格納されたＲＯＭ（Read Only Memory）１１と、ＣＰＵ１０のワークメモリとしてのＲＡＭ（Random Access Memory）１２と、

各種データや種々のコンテンツが格納されたハードディスク装置（ＨＤＤ）１３と、ＣＰＵ１０がネットワーク５（図１）を介して外部と通信するためのインターフェースであるネットワークインターフェース部１４と、フラッシュメモリ１５と、ハードディスク装置１３から音声情報でなるコンテンツが再生された場合に当該コンテンツに例えばＡＴＲＡＣ３（Adaptive Transform Acoustic Coding 3）の音声圧縮処理を行う符号化部１６と、圧縮符号化されたコンテンツに例えば公開鍵基盤（ＰＫＩ：Public-key Infrastructure）等による暗号化処理を施す暗号化部１７とを有し、これらがバスＢＵＳを介して相互に接続されることにより構成されている。

【００２４】

かかる構成に加えて、配信サーバ３は、フラッシュメモリ１５から読み出された各種情報に所定の拡散変調（例えばスペクトラム拡散変調等）処理を施す拡散変調部１９と、ハードディスク装置１３から与えられたコンテンツに拡散変調部１９から得られた後述する透かし情報を重畳させる重畳部１８とを有し、当該透かし情報が重畳されたコンテンツを後段の符号化部１６及び続く暗号化部１７に供給するようになされている。

【００２５】

まずＣＰＵ１０は、ネットワーク５（図１）を介してアクセスしてきた個人端末２から与えられるデータやコマンドをネットワークインターフェース部１４を介して取り込み、当該データやコマンドと、ＲＯＭ１１に格納されているソフトウェアとに基づいて各種処理を実行する。

【００２６】

そしてＣＰＵ１０は、この処理結果として、例えばハードディスク装置１３から読み出した所定のコンテンツや、他のプログラム又はコマンドなどのデータを、必要に応じて暗号化等した後にネットワークインターフェース部１４を介して対応する個人端末２に送出する。

【００２７】

このようにして配信サーバ３においては、アクセスしてきた個人端末２に対してコンテンツやこの他の必要なデータを送受信し得るようになされている。なお

配信サーバ３のハードディスク装置１３内にはそれぞれ複数のデータベース（図示せず）が格納されており、各種処理を実行するときに対応するデータベースから必要な情報を読み出し得るようになされている。

【００２８】

（１－３）個人端末の具体的構成

図３に、各個人端末２における本体部２Ｈの内部構成を示す。各個人端末２の本体部２Ｈは、全体の制御を司るＣＰＵ２０と、各種ソフトウェアが格納されたＲＯＭ２１と、ＣＰＵ２０のワークメモリとしてのＲＡＭ２２、各種データが格納されたハードディスク装置２３と、ＣＰＵ２０がネットワーク５（図１）を介して外部と通信するためのインターフェースであるネットワークインターフェース部２４と、スピーカ２５が接続された音声処理部２６と、ディスプレイ２７が接続された画像処理部２８と、キーボード２９及びマウス３０が接続されたインターフェース部３１と、ネットワークインターフェイス部２４を介して与えられたコンテンツにかけられた暗号を解除するデクリプト部３２とを有し、これらがバスＢＵＳを介して相互に接続されることにより構成されている。

【００２９】

かかる構成に加えて、各個人端末２の本体部２Ｈは、各個人端末２の本体部２Ｈは、デクリプト部３２において暗号が解除された後のコンテンツに重畳されている透かし情報を検出するＩＤ・フラグ検出部３４と、当該ＩＤ・フラグ検出部３２の検出結果に応じてコンテンツに所定の暗号をかける暗号化部３５と、必要に応じて暗号解除処理を行うと共に圧縮処理されたコンテンツを元の状態に復元するデクリプト／復号化部３６とを有する。

【００３０】

まずＣＰＵ２０は、ネットワーク５（図１）を介してアクセスしてきた配信サーバ３又は他の個人端末２から与えられるデータやコマンドをネットワークインターフェース部２６を介して取り込み、当該データやコマンドと、ＲＯＭ２１に格納されているソフトウェアとに基づいて各種処理を実行する。

【００３１】

そしてＣＰＵ２０は、この処理結果として、例えばハードディスク装置２３か

ら読み出した所定のコンテンツや他のプログラム又はコマンドなどのデータをネットワークインターフェース部２６を介して配信サーバ３又は対応する他の個人端末２に送出する。

【００３２】

このようにして個人端末２においては、アクセスしてきた配信サーバ３又は他の個人端末に対して、コンテンツやこの他の必要なデータを送受信し得るようになされている。なお個人端末２のハードディスク装置２３内にはそれぞれ複数のデータベース（図示せず）が格納されており、各種処理を実行するときに対応するデータベースから必要な情報を読み出し得るようになされている。

【００３３】

（１－４）監視サーバの具体的構成

さらに監視サーバ４の構成を図４に示す。この監視サーバ４は、監視サーバ４全体の制御を司るＣＰＵ４０と、各種ソフトウェアが格納されたＲＯＭ４１と、ＣＰＵ４０のワークメモリとしてのＲＡＭ４２と、各種データや種々のコンテンツが格納されたハードディスク装置４３と、ＣＰＵ４０がネットワーク５（図１）を介して外部と通信するためのインターフェースであるネットワークインターフェース部４４と、フラッシュメモリ４５と、ネットワーク５上を巡回しながら不正なコンテンツを検出する不正コンテンツ検出部４６とを有し、これらがバスＢＵＳを介して相互に接続されることにより構成されている。

【００３４】

この監視サーバ４内のハードディスク装置４３には、配信サーバ３に対して正規に登録した全ての個人端末２ごとにそれぞれ固有に割り当てられているユーザ識別情報X_{ID}を保有するデータベース(図示せず)が格納されている。

【００３５】

不正コンテンツ検出部４６は、例えばＷｉｎＭＸ及びグヌーテラ（Gnutella）等のファイル共有ソフトウェアを使用して、ネットワーク５（図１）上を巡回しながら各個人端末２から送信されるコンテンツを取得するようになされている。

【００３６】

そして不正コンテンツ検出部４６は、取得したコンテンツに付加されているユ

ーザ識別情報X_{ID}を検出して、コンテンツの発信元が正規登録したユーザの個人端末２に対応するユーザ識別情報X_{ID}と一致するか否かを判断した後、一致する場合もしない場合にも当該コンテンツを発信した個人端末２に対して所定の通知又は警告をネットワーク５を介して通知するようになされている。

【００３７】

（１－５）配信サーバから個人端末へのコンテンツ配信

実際にこのコンテンツ配信システム１において、図２に示す配信サーバ３のＣＰＵ１０は、個人端末２からアクセス要求があったとき、フラッシュメモリ１５から当該個人端末２を所有するユーザに割り当てられたユーザ識別情報（ＩＤ）X_{ID}と、当該ユーザ識別情報X_{ID}に付随して設けられた所定の判断用のフラグ（以下、これを格納定義フラグと呼ぶ）X_{FLG}とを読み出す。

【００３８】

この格納定義フラグX_{FLG}は、ユーザ側のデバイスである個人端末２内のハードディスク装置２３にコンテンツを格納する際に、当該コンテンツを暗号化するか否かを判断するためのフラグであり、ユーザ識別情報X_{ID}に付随して予めユーザによって立上り又は立下りが設定されている。

【００３９】

続いて、配信サーバ３のＣＰＵ１０は、フラッシュメモリ１５から読み出したユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を拡散変調部１９に送出する。拡散変調部１９は、ユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}に所定の拡散変調処理を施すようにして透かし情報X_{WM1}を生成する。

【００４０】

この透かし情報X_{WM1}は、いわゆる「電子透かし（Watermark）」と呼ばれる技術においてコンテンツの冗長部分に埋め込まれる著作権情報等であり、コンテンツの種類に応じてデータ内容が設定されるようになされている。

【００４１】

例えばコンテンツが音声情報でなる場合、透かし情報X_{WM1}は、一般に「強い音の直前直後の数10ミリ秒程度までにある微弱な音は強い音にかき消される」という人間の聴覚特性を利用することにより、当該コンテンツのうちの人間の聴

覚上重要でない部分に雑音として埋め込まれる。

【００４２】

この後、配信サーバ３のＣＰＵ１０は、拡散変調部１９において拡散変調した透かし情報X_{WM1}と、ハードディスク装置１３から再生したユーザが所望するコンテンツＤ１とを重畳部１８において重畳させるようにして合成情報データＤ２を生成する。

【００４３】

具体的に合成情報データＤ２は、上述した電子透かしの技術に基づいて、コンテンツＤ１である音声情報を所定の標本化周波数（例えば44.1〔kHz〕）で標本化した後、下位ビットを探索して透かし情報X_{WM1}を埋め込む手法や、フーリエ変換やウェーブレット変換を用いて音声情報であるコンテンツＤ１の波形分析を行った後に特定の周波数成分に透かし情報X_{WM1}を埋め込む手法などにより生成される。

【００４４】

続いて配信サーバ３のＣＰＵ１０は、重畳部１８から得られた合成情報データＤ２を符号化部１６に送出して圧縮符号化させた後、続く暗号化部１７において所定の暗号（以下、これを第１の暗号と呼ぶ）で暗号化させる。

【００４５】

この後配信サーバ３のＣＰＵ１０は、暗号化部１７において暗号化した圧縮情報データ（以下、これを配信用コンテンツデータと呼ぶ）Ｄ３をネットワークインターフェイス部１４を介してネットワーク５上に接続された対応する個人端末２に送信する。

【００４６】

一方、このコンテンツ配信システム１において、図３に示す個人端末のＣＰＵ２０は、図５に示すコンテンツ受信処理手順ＲＴ１をステップＳＰ０から開始し、ネットワーク５（図１）を介して配信サーバ３から送信された配信用コンテンツデータＤ３をネットワークインターフェイス部２４を介してデクリプト部３２に送出する（ステップＳＰ１）。

【００４７】

このとき個人端末２のＣＰＵ２０は、配信用コンテンツデータＤ３にユーザ識別情報X_{ID}が付加されているか否かを判断し（ステップＳＰ２）、当該ユーザ識別情報X_{ID}が存在する場合のみ、デクリプト部３２において上述の第１の暗号を解除するための暗号解除処理を継続する（ステップＳＰ３）。

【００４８】

一方、個人端末２のＣＰＵ２０は、配信用コンテンツデータＤ３にユーザ識別情報X_{ID}が付加されていないと判断した場合には、第１の暗号を解除しない旨を画像処理部２８を介してディスプレイ２７上に画面表示させるようにしてユーザに通知する（ステップＳＰ４）。

【００４９】

そして個人端末２のＣＰＵ２０、デクリプト部３２において暗号解除した配信用コンテンツデータ（以下、これを圧縮コンテンツデータと呼ぶ）Ｄ４を、ＩＤ・フラグ検出部３４及び暗号化部３５にそれぞれ送出する。

【００５０】

ＩＤ・フラグ検出部３４は、圧縮コンテンツデータＤ４に埋め込まれている透かし情報X_{WM1}に逆拡散変調処理を施すことにより、当該透かし情報X_{WM1}からユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を抽出する。

【００５１】

その際、個人端末２のＣＰＵ２０は、ＲＡＭ２２から当該個人端末２に割り当てられているユーザ識別情報X_{ID}を読み出して、これをＩＤ・フラグ検出部３４において抽出されたユーザ識別情報X_{ID}と照合して両者が一致するか否かを判断する（ステップＳＰ５）。

【００５２】

この判断結果が肯定的な場合には、個人端末２のＣＰＵ２０は、ＩＤ・フラグ検出部３４から抽出された格納定義フラグX_{FLG}に基づいて、当該格納定義フラグX_{FLG}の立上り又は立下りを検出し、当該検出結果に応じて、デクリプト部３４から送出される圧縮コンテンツデータＤ４を暗号化するか否かを判断する（ステップＳＰ６）。

【００５３】

これに対してユーザ識別情報X_{ID}の照合判断結果が否定的な場合には、個人端末２のＣＰＵ２０は、コンテンツの受信が不可である旨を画像処理部２８を介してディスプレイ２７上に画面表示させるようにしてユーザに通知する（ステップＳＰ７）。

【００５４】

やがて暗号化部３５は、個人端末２のＣＰＵ２０から得られる格納定義フラグX_{FLG}に応じた暗号化の有無結果に基づいて、暗号化する旨が得られた場合のみ、デクリプト部３２から与えられた圧縮コンテンツデータＤ４に所定の暗号（以下、これを第２の暗号と呼ぶ。この暗号は第１の暗号と同一であってもよい。）をかける（ステップＳＰ８）。

【００５５】

続いて個人端末２のＣＰＵ２０は、暗号化部３５において必要に応じて第２の暗号がかけられた圧縮コンテンツデータＤ５をハードディスク装置２３に格納する（ステップＳＰ９）。

【００５６】

この後、個人端末２のＣＰＵ２０は、ユーザからマウス又はキーボード等による操作に基づく再生要求があったとき、ハードディスク装置２３から対応する圧縮コンテンツデータＤ５を再生してデクリプト／復号化部３６に送出する。

【００５７】

デクリプト／復号化部３６は、ハードディスク装置２３から再生された圧縮コンテンツデータＤ５にかけられている第２の暗号を解除した後、圧縮処理された圧縮コンテンツデータＤ４を元の状態であるコンテンツＤ１に復元する（ステップＳＰ１０）。

【００５８】

かくして個人端末２のＣＰＵ２０は、デクリプト／復号化部３６から得られた元のコンテンツＤ１を音声処理部２６を介してスピーカ２５から放音するようにしてユーザに提供する（ステップＳＰ１１）。

【００５９】

（１－６）第１の実施の形態による動作及び効果

以上の構成において、このコンテンツ配信システム１では、配信サーバ３は、個人端末２からアクセス要求があったとき、当該個人端末２のユーザに関するユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を読み出して拡散変調することにより透かし情報X_{WM1}を生成する。

【００６０】

続いて配信サーバ３は、透かし情報X_{WM1}を指定されたコンテンツＤ１に埋め込んだ後、第１の暗号をかけるようにして配信用コンテンツデータＤ３を生成し、これをネットワーク５を介してアクセス要求のあった個人端末２に送信する。

【００６１】

かかる個人端末,2では、配信サーバ３から送信される配信用コンテンツデータＤ３について、ユーザ識別情報X_{ID}の存在を条件として第１の暗号を解除した後、圧縮コンテンツデータＤ４に埋め込まれている透かし情報X_{WM1}からユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を抽出する。

【００６２】

そして個人端末２は、抽出したユーザ識別情報X_{ID}が、配信サーバ３への登録時に当該個人端末２に割り当てられたユーザ識別情報X_{ID}と一致し、かつ当該格納定義フラグX_{FLG}が立上り状態である場合のみ、透かし情報X_{WM1}が埋め込まれた圧縮コンテンツデータＤ４に第２の暗号をかけた後、ハードディスク装置２３に格納する。

【００６３】

このようにして個人端末２において、ネットワーク５を介して配信サーバ３からコンテンツを受信した際に、当該個人端末２内のハードディスク装置２３には、コンテンツがユーザ識別情報X_{ID}を透かし情報X_{WM1}として埋め込まれた状態で格納されることにより、後にハードディスク装置２３から当該コンテンツが外部に取り出された場合でも、常にユーザ識別情報X_{ID}が付随することとなり、この結果、かかるコンテンツが不正に取得したものか否かを判断することができる。

【００６４】

以上の構成によれば、コンテンツ配信システム１では、配信サーバ３において、ユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を透かし情報として埋め込んだコンテンツに第１の暗号をかけてアクセス要求のあった個人端末２にネットワークを介して送信する一方、当該個人端末２において、受信したコンテンツを、ユーザ識別情報X_{ID}が存在した場合のみ第１の暗号を解除した後、当該ユーザ識別情報X_{ID}が有効であり、かつ当該格納定義フラグX_{FLG}が立上り状態である場合のみハードディスク装置２３に格納するようにしたことにより、後にハードディスク装置２３から当該コンテンツが外部に取り出された場合でも、常にユーザ識別情報X_{ID}が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信システム１を実現することができる。

【００６５】

（２）第２の実施の形態

（２－１）第２の実施の形態におけるコンテンツ配信システムの全体構成

図６は、第２の実施の形態におけるコンテンツ配信システム５０を示し、図１に示す第１の実施の形態におけるコンテンツ配信システム１とは、各個人端末５１（51_1～51_n）及び配信サーバ５２の構成が異なることを除いて同様に構成されている。

【００６６】

（２－２）第２実施の形態による配信サーバ及び個人端末の具体的構成

図７は第２の実施の形態による配信サーバ５２を示し、図２に示す配信サーバ３とは、拡散変調部１９（図２）が取り除かれる以外は当該配信サーバ３と同様に構成されている。

【００６７】

この配信サーバ５２では、ＣＰＵ１０がフラッシュメモリ１５から読み出したユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を重畳部１８において、ハードディスク装置１３から再生されたコンテンツＤ１に重畳させた後、符号化部１６及び続く暗号化部１７に供給するようになされている。

【００６８】

また図８は第２の実施の形態による個人端末５１を示し、図３に示す個人端末２とは、本体部５１Ｈ内において拡散変調部５５及び重畳部５６が加えられたことを除いて、当該個人端末２と同様に構成されている。

【００６９】

この個人端末５１では、配信サーバ５２（図７）においてユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を「電子透かし」によるコンテンツへの埋め込み対象としなかった分、当該個人端末５１において拡散変調部５５がユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を拡散変調処理した後、重畳部５６においてコンテンツの冗長部分に埋め込むようになされている。

【００７０】

（２－３）配信サーバから個人端末へのコンテンツ配信

実際に図７に示す配信サーバ５２のＣＰＵ１０は、個人端末５１（図６）からアクセス要求があったとき、フラッシュメモリ１５から当該個人端末５１を所有するユーザに割り当てられたユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を読み出す。

【００７１】

続いて、配信サーバ５２のＣＰＵ１０は、フラッシュメモリ１５から読み出したユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}と、ハードディスク装置１３から再生したユーザが所望するコンテンツＤ１とを重畳部１８において重畳させるようにして合成情報データＤ１０を生成する。

【００７２】

具体的に合成情報データＤ１０は、上述した電子透かしの技術とは異なり、コンテンツＤ１を構成する音声データ群のデータフォーマット内のヘッダ部分に書き込むことで生成されるようになされている。

【００７３】

続いて配信サーバ５２のＣＰＵ１０は、重畳部１８から得られた合成情報データＤ１０を符号化部１６に送出して圧縮符号化させた後、続く暗号化部１７において第１の暗号で暗号化させる。

【００７４】

この後配信サーバ５２のＣＰＵ１０は、暗号化部１７において暗号化した配信用コンテンツデータＤ１１をネットワークインターフェイス部１４を介してネットワーク５上に接続された対応する個人端末５１（図６）に送信する。

【００７５】

一方、図６に示す個人端末５１のＣＰＵ２０は、図９に示すコンテンツ受信処理手順ＲＴ２をステップＳＰ２０から開始し、ネットワーク５（図１）を介して配信サーバ５２から送信された配信用コンテンツデータＤ１１をネットワークインターフェイス部２４を介してデクリプト部３２に送出する（ステップＳＰ２１）。

【００７６】

このとき個人端末５１のＣＰＵ２０は、配信用コンテンツデータＤ１１にユーザ識別情報X_{ID}が付加されているか否かを判断し（ステップＳＰ２２）、当該ユーザ識別情報X_{ID}が存在する場合のみ、デクリプト部３２において上述の第１の暗号を解除するための暗号解除処理を行う（ステップＳＰ２３）。

【００７７】

一方、個人端末５１のＣＰＵ２０は、配信用コンテンツデータＤ１１にユーザ識別情報X_{ID}が付加されていないと判断した場合には、第１の暗号を解除しない旨を画像処理部２８を介してディスプレイ２７上に画面表示させるようにしてユーザに通知する（ステップＳＰ２４）。

【００７８】

そして個人端末５１のＣＰＵ２０は、デクリプト部３２において暗号解除された圧縮コンテンツデータＤ１２を、ＩＤ・フラグ検出部３４及び重畳部３５にそれぞれ送出する。

【００７９】

ＩＤ・フラグ検出部３４は、圧縮コンテンツデータＤ１２からユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を抽出する。その際、個人端末５１のＣＰＵ２０は、ＲＡＭ２２から当該個人端末５１に割り当てられているユーザ識別情報X_{ID}を読み出して、これをＩＤ・フラグ検出部３４において抽出されたユーザ

識別情報X_{ID}と照合して両者が一致するか否かを判断する（ステップＳＰ２５）。

【００８０】

この判断結果が肯定的な場合には、個人端末５１のＣＰＵ２０は、ＩＤ・フラグ検出部３４において抽出したユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}のうち、ユーザ識別情報X_{ID}を拡張変調部５５に送出させる一方、格納定義フラグX_{FLG}を暗号化部３５に送出させる（ステップＳＰ２６）。

【００８１】

これに対してユーザ識別情報X_{ID}の照合判断結果が否定的な場合には、個人端末５１のＣＰＵ２０は、コンテンツの受信が不可である旨を画像処理部２８を介してディスプレイ２７上に画面表示させるようにしてユーザに通知する（ステップＳＰ２７）。

【００８２】

拡散変調部５５は、ＩＤ・フラグ検出部３４から与えられたユーザ識別情報X_{ID}に所定の拡散変調処理を施すようにして透かし情報X_{WM2}を生成する。この後、個人端末５１のＣＰＵ２０は、拡散変調部５５において拡散変調した透かし情報X_{WM2}と、デクリプト部３２から送出される圧縮コンテンツデータＤ１２とを重畳部５６において重畳させるようにして合成圧縮コンテンツデータＤ１３を生成する（ステップＳＰ２６）。

【００８３】

続いて個人端末５１のＣＰＵ２０は、ＩＤ・フラグ検出部３４から抽出された格納定義フラグX_{FLG}に基づいて、当該格納定義フラグX_{FLG}の立上り又は立下りを検出し、当該検出結果に応じて、重畳部５６から送出される合成圧縮コンテンツデータＤ１３を暗号化するか否かを判断する（ステップＳＰ２８）。

【００８４】

やがて暗号化部３５は、個人端末５１のＣＰＵ２０から得られる格納定義フラグX_{FLG}に応じた暗号化の有無結果に基づいて、暗号化する旨が得られた場合のみ、重畳部５６から送出される合成圧縮コンテンツデータＤ１３に第２の暗号をかける（ステップＳＰ２９）。

【００８５】

これに対して暗号化しない旨が得られた場合には、暗号化部３５は、第２の暗号をかけることなく、重畳部５６から送出される合成圧縮コンテンツデータＤ１３をそのままハードディスク装置２３に格納する（ステップＳＰ３０）。

【００８６】

続いて個人端末５１のＣＰＵ２０、暗号化部３５において必要に応じて第２の暗号がかけられた合成圧縮コンテンツデータＤ１４をハードディスク装置２３に格納する（ステップＳＰ３０）。

【００８７】

この後、個人端末５１のＣＰＵ２０は、ユーザからマウス２９又はキーボード３０等による操作に基づく再生要求があったとき、ハードディスク装置２３から対応する合成圧縮コンテンツデータＤ１４を再生してデクリプト／復号化部３６に送出する。

【００８８】

デクリプト／復号化部３６は、ハードディスク装置２３から再生された合成圧縮コンテンツデータＤ１４にかけられている第２の暗号を解除した後、圧縮処理された合成圧縮コンテンツデータＤ１３を元の状態であるコンテンツＤ１に復元する（ステップＳＰ３１）。

【００８９】

かくして個人端末５１のＣＰＵ２０、デクリプト／復号化部３６から得られた元のコンテンツＤ１を音声処理部２６を介してスピーカ２５から放音するようにしてユーザに提供する（ステップＳＰ３２）。

【００９０】

（２－４）第２の実施の形態による動作及び効果

以上の構成において、このコンテンツ配信システム５０では、配信サーバ５２は、個人端末５１からアクセス要求があったとき、当該個人端末５１のユーザに関するユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を読み出した後、指定されたコンテンツＤ１に重畳させて第１の暗号をかけるようにして配信用コンテンツデータＤ１１を生成し、これをネットワーク５を介してアクセス要求のあっ

た個人端末５１に送信する。

【００９１】

かかる個人端末５１では、配信サーバ５２から送信される配信用コンテンツデータＤ１１について、ユーザ識別情報X_{ID}の存在を条件として第１の暗号を解除した後、圧縮コンテンツデータＤ１２からユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を抽出する。

【００９２】

続いて個人端末５１は、抽出したユーザ識別情報X_{ID}が、ＲＡＭ２２に格納されている当該個人端末５１に割り当てられたユーザ識別情報X_{ID}と一致する場合のみ、当該ユーザ識別情報X_{ID}を拡散変調することにより透かし情報X_{WM2}を生成すると共に、格納定義フラグX_{FLG}の立上り状態を判断する。

【００９３】

そして個人端末５１は、格納定義フラグX_{FLG}が立上り状態である場合のみ、透かし情報X_{WM2}を圧縮コンテンツデータＤ１２に埋め込むようにして合成圧縮コンテンツデータＤ１３を生成し、さらに当該合成圧縮コンテンツデータＤ１３に第２の暗号をかけた後、ハードディスク装置２３に格納する。

【００９４】

このようにして個人端末５１において、ネットワーク５を介して配信サーバ５２からコンテンツを受信した際に、当該個人端末５１内のハードディスク装置２３には、ユーザ識別情報X_{ID}の有効性及び格納定義フラグX_{FLG}の立上り状態を条件として当該ユーザ識別情報X_{ID}を透かし情報X_{WM2}としてコンテンツに埋め込んだ状態で格納することにより、後にハードディスク装置２３から当該コンテンツが外部に取り出された場合でも、常にユーザ識別情報X_{ID}が付随することとなり、この結果、かかるコンテンツが不正に取得したものか否かを判断することができる。

【００９５】

以上の構成によれば、コンテンツ配信システム５０では、配信サーバ３において、ユーザ識別情報X_{ID}を重畳したコンテンツに第１の暗号をかけてアクセス要求のあった個人端末２にネットワークを介して送信する一方、当該個人端末２

において、受信したコンテンツを、ユーザ識別情報X_{ID}が存在した場合のみ第１の暗号を解除した後、当該ユーザ識別情報X_{ID}が有効であり、かつ格納定義フラグX_{FLG}が立上り状態である場合のみ当該ユーザ識別情報X_{ID}を透かし情報X_{WM2}としてコンテンツに埋め込んだ状態でハードディスク装置２３に格納するようにしたことにより、後にハードディスク装置２３から当該コンテンツが外部に取り出された場合でも、常にユーザ識別情報X_{ID}が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信システム５０を実現することができる。

【００９６】

（３）第３の実施の形態

（３－１）第３の実施の形態によるコンテンツ配信システムの構成

第３の実施の形態におけるコンテンツ配信システム（図示せず）は、図６に示す第２の実施の形態におけるコンテンツ配信システム５０とは、各個人端末６０（60_1～60_n）の構成が異なることを除いて同様に構成されている。

【００９７】

ここで図１０に第３の実施の形態による個人端末６０を示し、図８に示す個人端末５１とは、本体部６０Ｈ内においてＩＤ・フラグ検出部３４及び暗号化部３５に代えて、フラグ検出部６１及び書込み部６２が設けられていることを除いて、当該個人端末５１とほぼ同様に構成されている。

【００９８】

この個人端末６０では、上述した第２の実施の形態における個人端末５１のようにコンテンツにユーザ識別情報X_{ID}を埋め込ませた後にハードディスク装置に格納させるのではなく、先にハードディスク装置にコンテンツを格納しておき、その後当該ハードディスク装置から再生したコンテンツにユーザ識別情報X_{ID}を埋め込ませるようになされている。

【００９９】

（３－２）配信サーバから個人端末へのコンテンツ配信

図１０に示す個人端末６０のＣＰＵ２０は、図１１に示すコンテンツ受信処理手順ＲＴ３をステップＳＰ４０から開始し、ネットワーク５（図１）を介して配信サーバ５２から送信された配信用コンテンツデータＤ１１をネットワークインターフェイス部２４を介してハードディスク装置２３に格納する（ステップＳＰ４１及びＳＰ４２）。

【０１００】

この後、個人端末６０のＣＰＵ２０は、ユーザからマウス２９又はキーボード３０等による操作に基づく再生要求があったとき、ハードディスク装置２３から対応する配信用コンテンツデータＤ１１を再生してデクリプト部３２に送出する（ステップＳＰ４３）。

【０１０１】

このとき個人端末６０のＣＰＵ２０は、配信用コンテンツデータＤ１１にユーザ識別情報X_{ID}が付加されているか否かを判断し（ステップＳＰ４４）、当該ユーザ識別情報X_{ID}が存在する場合のみ、デクリプト部３２において上述の第１の暗号を解除するための暗号解除処理を行う（ステップＳＰ４５）。

【０１０２】

一方、個人端末６０のＣＰＵ２０は、配信用コンテンツデータＤ１１にユーザ識別情報X_{ID}が付加されていないと判断した場合には、第１の暗号を解除しない旨を画像処理部２８を介してディスプレイ２７上に画面表示させるようにしてユーザに通知する（ステップＳＰ４６）。

【０１０３】

続いてデクリプト部３２は、第１の暗号を解除した後の圧縮処理された圧縮コンテンツデータＤ１２をフラグ検出部６１及び重畳部５６に送出する。フラグ検出部６１は、圧縮コンテンツデータＤ１２から格納定義フラグX_{FLG}を抽出して重畳部５６に送出する。

【０１０４】

個人端末６０のＣＰＵ２０は、ＲＡＭ２２から当該個人端末６０に割り当てられているユーザ識別情報X_{ID}を読み出して、拡散変調部５５において拡散変調させた後、透かし情報X_{WM3}として重畳部５６に送出させる。

【０１０５】

個人端末６０のＣＰＵ２０は、拡散変調部５５において拡散変調した透かし情報X_{WM3}と、デクリプト部３２から送出される圧縮コンテンツデータＤ１２と、フラグ検出部６１から送出される格納定義フラグX_{FLG}とを重畳部５６において重畳させるようにして合成圧縮コンテンツデータＤ１５を生成する。

【０１０６】

具体的に合成情報データＤ１５は、上述した電子透かしの技術を用いて透かし情報X_{WM3}がコンテンツに埋め込まれると共に、格納定義フラグX_{FLG}がコンテンツを構成する音声データ群のデータフォーマット内のヘッダ部分に書き込むことで生成されるようになされている。

【０１０７】

続いて個人端末６０のＣＰＵ２０は、重畳部５６から得られたが合成情報データＤ１５を書込み部６２を介してハードディスク装置２３に格納させる。その際、個人端末６０のＣＰＵ２０は、ハードディスク装置２３において、既に格納されている元の配信用コンテンツデータＤ１１を消去して、新たに合成情報データＤ１５を書き直す。

【０１０８】

この後、個人端末６０のＣＰＵ２０は、ユーザからマウス２９又はキーボード３０等による操作に基づく再生要求があったとき、ハードディスク装置２３から対応する合成情報データＤ１５を再生してデクリプト／復号化部３６に送出する。

【０１０９】

デクリプト／復号化部３６は、ハードディスク装置２３から再生された圧縮処理されている合成情報データＤ１５を元の状態であるコンテンツＤ１に復元する。

【０１１０】

かくして個人端末６０のＣＰＵ２０、デクリプト／復号化部３６から得られた元のコンテンツＤ１を音声処理部２６を介してスピーカ２５から放音するようにしてユーザに提供する。

【０１１１】

（３－３）第３の実施の形態による動作及び効果

以上の構成において、このコンテンツ配信システムでは、配信サーバ５２は、個人端末６０からアクセス要求があったとき、当該個人端末６０のユーザに関するユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を読み出した後、指定されたコンテンツＤ１に重畳させて第１の暗号をかけるようにして配信用コンテンツデータＤ１１を生成し、これをネットワーク５を介してアクセス要求のあった個人端末６０に送信する。

【０１１２】

かかる個人端末６０では、配信サーバ５２から送信される配信用コンテンツデータＤ１１を一旦ハードディスク装置２３に格納しておき、必要に応じて当該ハードディスク装置２３から配信用コンテンツデータＤ１１を再生した後、ユーザ識別情報X_{ID}の存在を条件として第１の暗号を解除する。

【０１１３】

続いて個人端末６０は、第１の暗号が解除された圧縮コンテンツデータＤ１２から格納定義フラグX_{FLG}を抽出した後、ＲＡＭ２２に格納されている当該個人端末５１に割り当てられたユーザ識別情報X_{ID}を拡散変調することにより透かし情報X_{WM3}を生成する。

【０１１４】

そして個人端末６０は、透かし情報X_{WM3}と圧縮コンテンツデータＤ１２と格納定義フラグX_{FLG}とを重畳させて合成圧縮コンテンツデータＤ１５を生成した後、これをハードディスク装置２３に格納する。

【０１１５】

このようにして個人端末６０において、ネットワーク５を介して配信サーバ５２からコンテンツを受信した際に、当該個人端末６０内のハードディスク装置２３には、一旦当該コンテンツを格納した後、必要に応じて再生した際に、ユーザ識別情報X_{ID}を透かし情報X_{WM3}としてコンテンツに埋め込んだ状態で再度格納することにより、後にハードディスク装置２３から当該コンテンツが外部に取り出された場合でも、常にユーザ識別情報X_{ID}が付随することとなり、この

結果、かかるコンテンツが不正に取得したものか否かを判断することができる。

【０１１６】

以上の構成によれば、コンテンツ配信システム１では、配信サーバ３において、ユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を重畳したコンテンツに第１の暗号をかけてアクセス要求のあった個人端末２にネットワークを介して送信する一方、当該個人端末２において、受信したコンテンツを一旦当該コンテンツを格納した後、必要に応じて再生した際に、ユーザ識別情報X_{ID}が存在した場合のみ第１の暗号を解除した後、ユーザ識別情報X_{ID}を透かし情報X_{WM3}としてコンテンツに埋め込んだ状態で再度格納することにより、後にハードディスク装置２３から当該コンテンツが外部に取り出された場合でも、常にユーザ識別情報X_{ID}が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信システムを実現することができる。

【０１１７】

（４）第１～第３の実施の形態における監視サーバによる警告

（４－１）異なるユーザに基づくコンテンツ監視処理

上述した第１～第３の実施の形態において、図４に示す監視サーバ４は、ネットワーク５上を巡回しながら各個人端末２から送信されるコンテンツを取得し、当該コンテンツの発信元が正規登録したユーザの個人端末２であるか否かを検出して、当該検出結果に応じた通知又は警告をコンテンツを発信した個人端末に送信する。

【０１１８】

実際に監視サーバ４のＣＰＵ４０は、図１２に示すコンテンツ監視処理手順ＲＴ４をステップＳＰ６０から開始し、続くステップＳＰ６１に進んで、ネットワーク５を介して各個人端末からそれぞれコンテンツ（コンテンツ配信データ）を取得する。

【０１１９】

監視サーバ４のＣＰＵ４０は、ステップＳＰ６２において、取得したコンテン

ツ（コンテンツ配信データ）にユーザ識別情報X_{ID}が付加されているか否かを判断し、当該ユーザ識別情報X_{ID}が存在する場合のみ、ステップＳＰ６３に進んで、ネットワーク５を介して配信サーバから当該コンテンツの発信元である個人端末に割り当てられているユーザ識別情報X_{ID}を取得する。

【０１２０】

監視サーバ４のＣＰＵ４０は、ステップＳＰ６４に進んで、不正コンテンツ検出部４６において、コンテンツ（コンテンツ配信データ）から得られたユーザ識別情報X_{ID}と、配信サーバから取得したユーザ識別情報X_{ID}とを照合して両者が一致するか否かを判断する。

【０１２１】

このステップＳＰ６４における判断結果が肯定的な場合には、コンテンツの発信元である個人端末が当該コンテンツの配信を正規に登録しているユーザがもつ個人端末であることを表しており、このとき監視サーバ４のＣＰＵ４０は、ステップＳＰ６５に進んで、不正コンテンツ検出部４６において、例えば「あなたが所有するコンテンツがネットワーク上に流出していますよ。」のような所定の通知が記述された通知データをネットワークを介して正規登録しているユーザがもつ個人端末に送信する。

【０１２２】

この後、監視サーバ４のＣＰＵ４０は再度ステップＳＰ６１に戻って、上述と同様にネットワーク５上を巡回しながら不正なコンテンツの流出を検出し続ける。

【０１２３】

これに対してステップＳＰ６４における判断結果が否定的な場合には、コンテンツの発信元である個人端末が当該コンテンツの配信を正規に登録しているユーザがもつ個人端末と異なることを表しており、このとき監視サーバ４のＣＰＵ４０は、ステップＳＰ６６に進んで、不正コンテンツ検出部４６において、例えば「あなたは他人のコンテンツを不正にネットワーク５上に流出させており、かかる行為は著作権法に違反しているため罰せられますよ。」のような所定の警告が記述された警告データをネットワークを介して当該コンテンツを発信した個人端

末に送信する。

【０１２４】

この後、監視サーバ４のＣＰＵ４０は再度ステップＳＰ６１に戻って、上述と同様にネットワーク５上を巡回しながら不正なコンテンツの流出を検出し続ける。

【０１２５】

このように監視サーバ４では、各個人端末２から発信されるコンテンツをネットワーク５上を常時巡回しながら監視し、ネットワーク５上に流出したコンテンツを検出した場合には、当該コンテンツを発信した個人端末２に対して所定の通知又は警告を発信することにより、当該コンテンツの発信者にその旨を認識させることができ、かくしてネットワーク５上に流出したコンテンツの著作権が侵害されるのを未然に防止することができる。

【０１２６】

（４－２）ファイル共有に基づくコンテンツ監視処理

上述した第１～第３の実施の形態において、図４に示す監視サーバ４は、ネットワーク５上を巡回しながら各個人端末から送信されるコンテンツを取得し、共有ファイルを提供するユーザの個人端末が当該コンテンツの発信元が正規登録したユーザの個人端末であるか否かを検出して、当該検出結果に応じた通知又は警告をコンテンツを発信した個人端末に送信する。

【０１２７】

実際に監視サーバ４のＣＰＵ４０は、図１３に示すコンテンツ監視処理手順ＲＴ５をステップＳＰ７０から開始し、続くステップＳＰ７１に進んで、ファイル共有ソフトウェアを使用して、ネットワーク５を介して各個人端末からそれぞれコンテンツ（コンテンツ配信データ）を取得する。

【０１２８】

監視サーバ４のＣＰＵ４０は、ステップＳＰ７２において、取得したコンテンツ（コンテンツ配信データ）にユーザ識別情報X_{ID}が付加されているか否かを判断し、当該ユーザ識別情報X_{ID}が存在する場合のみ、ステップＳＰ７３に進んで、取得したコンテンツから共有ファイルに基づくＩＰアドレス、ＭＡＣアド

レス及び日時等の関連情報を取得した後、ステップＳＰ７４に進んで、当該関連情報をネットワーク５を介して配信サーバに送信する。

【０１２９】

やがて監視サーバ４のＣＰＵ４０は、ステップＳＰ７５に進んで、ネットワーク５を介して配信サーバから当該コンテンツの発信元である個人端末に割り当てられているユーザ識別情報X_{ID}を取得した後、ステップＳＰ７６に進んで、不正コンテンツ検出部４６において、当該取得したユーザ識別情報X_{ID}と、コンテンツ（コンテンツ配信データ）から得られたユーザ識別情報X_{ID}とを照合して両者が一致するか否かを判断する。

【０１３０】

このステップＳＰ７６における判断結果が肯定的な場合には、コンテンツの発信元である個人端末が当該コンテンツの配信を正規に登録しているユーザがもつ個人端末であることを表しており、このとき監視サーバ４のＣＰＵ４０は、ステップＳＰ７７に進んで、不正コンテンツ検出部４６において、例えば「あなたが所有するコンテンツがネットワーク上に流出していますよ。」のような所定の通知が記述された通知データをネットワーク５を介して正規登録しているユーザがもつ個人端末に送信する。

【０１３１】

この後、監視サーバ４のＣＰＵ４０は再度ステップＳＰ７１に戻って、上述と同様にネットワーク５上を巡回しながら不正なコンテンツの流出を検出し続ける。

【０１３２】

これに対してステップＳＰ７６における判断結果が否定的な場合には、コンテンツの発信元である個人端末が当該コンテンツの配信を正規に登録しているユーザがもつ個人端末と異なることを表しており、このとき監視サーバ４のＣＰＵ４０は、ステップＳＰ７８に進んで、不正コンテンツ検出部４６において、例えば「あなたは他人のコンテンツを不正にネットワーク上に流出させており、かかる行為は著作権法に違反しているため罰せられますよ。」のような所定の警告が記述された警告データをネットワーク５を介して当該コンテンツを発信した個人端

末に送信する。

【０１３３】

この後、監視サーバ４のＣＰＵ４０は再度ステップＳＰ７１に戻って、上述と同様にネットワーク５上を巡回しながら不正なコンテンツの流出を検出し続ける。

【０１３４】

このように監視サーバ４では、各個人端末２から発信されるコンテンツをネットワーク５上を常時巡回しながら監視し、ネットワーク５上に流出したコンテンツを検出した場合には、当該コンテンツを発信した共有ファイルを提供するユーザの個人端末２に対して所定の通知又は警告を発信することにより、当該コンテンツの発信者にその旨を認識させることができ、かくしてネットワーク５上に流出したコンテンツの著作権が侵害されるのを未然に防止することができる。

【０１３５】

（５）他の実施の形態

なお上述のように第１～第３の実施の形態においては、本発明を図１及び図６のように構成された各個人端末（端末装置）２、５１、６０及び配信サーバ３、５２からなるコンテンツ配信システム１、５０に適用するようにした場合について述べたが、本発明はこれに限らず、これ以外の形態のこの他種々の構成のコンテンツ配信システムに広く適用することができる。

【０１３６】

さらに上述のように第１～第３の実施の形態においては、各個人端末（端末装置）２、５１、６０及び配信サーバ３、５２間では、インターネット等のネットワーク５を介して相互に接続するようにした場合について述べたが、本発明はこれに限らず、これ以外にも一般公衆回線やＬＡＮ（Local Area Network）等の有線通信回線網のみならず無線通信回線網からなるネットワークに広く適用することができる。

【０１３７】

また各個人端末（端末装置）２、５１、６０及び配信サーバ３、５２間では、ネットワークを介することなく、配信サーバ３、５２から各個人端末（端末装置

）２、５１、６０にコンテンツをいわゆるパッケージメディア（既製品のメディア）として送付するようにしても良い。この場合、ユーザは、予め個人端末の購入時、メディアの購入時又はコンテンツの使用前までに、固有のユーザ識別情報を本人認証を前提として配信サーバに登録しておき、当該配信サーバで管理するようにしておく必要がある。その際、配信サーバは、必要に応じてユーザ識別情報を暗号化しておき、使用時にユーザ認証を行わせるようにしても良い。

【０１３８】

さらに上述の第１～第３の実施の形態においては、配信サーバ３、５２においてコンテンツに暗号（第１の暗号）をかけて送信する一方、個人端末（端末装置）２、５１、６０においてユーザ識別情報X_{ID}の存在を条件として当該コンテンツから暗号（第１の暗号）を解除した後、当該ユーザ識別情報X_{ID}が有効であり、かつ格納定義フラグX_{FLG}が立上り状態である場合のみ当該コンテンツに第２の暗号をかけてハードディスク装置（格納手段）２３に格納するようにした場合について述べたが、本発明はこれに限らず、このような個人端末（端末装置）２、５１、６０側で再暗号化することなく、個人端末（端末装置）２、５１、６０において、配信サーバ３、５２から受信したコンテンツにかけられている暗号（第１の暗号）をユーザ識別情報X_{ID}及び又は格納定義フラグX_{FLG}に基づいて暗号解除して格納するか否かを判断した後でハードディスク装置（格納手段）２３に格納するようにしても良い。

【０１３９】

さらに上述の第１～第３の実施の形態においては、配信サーバ３、５２でコンテンツに付加される格納定義フラグX_{FLG}を、個人端末（端末装置）２、５１、６０において暗号の解除又は非解除の判断基準とするようにした場合について述べたが、本発明はこれに限らず、個人端末（端末装置）２、５１、６０を所有するユーザの選択に応じて暗号の解除又は非解除を決定するようにしても良いし、併用するようにしても構わない。この場合、暗号の解除又は非解除は、ユーザごと及び又はコンテンツごとに設定するようにしても良い。

【０１４０】

さらに上述の第１～第３の実施の形態においては、配信サーバ３、５２又は個

人端末（端末装置）２、５１、６０でユーザ識別情報X_{ID}を、例えばスペクトラム拡散変調等の拡散変調処理により電子透かし（Watermark）と呼ばれる透かし情報に変換するようにした場合について述べたが、本発明はこれに限らず、要はコンテンツに著作権情報として埋め込むことができれば、この他例えばステガノグラフィ（Steganograpy）等の暗号技術を適用するようにしても良い。

【０１４１】

さらに上述の第１～第３の実施の形態においては、配信サーバ３、５２に登録されるユーザ識別情報X_{ID}として、個人端末（端末装置）２、５１、６０を所有するユーザに割り当てられたユーザＩＤを適用するようにした場合について述べたが、本発明はこれに限らず、ＩＰｖ６（internet protocol version ６）やＩＰｖ４（internet protocol version ４）等のインターネット・プロトコルのバージョンで表現されるＩＰアドレス、パスワード、プロバイダ名、電子メールアドレス、さらには公的機関又はそれに順ずる機関が発行するＩＤや証明書番号、日時、国名、電話番号、端末装置名及び製造時のシリアル番号や機器ＩＤ等を広く適用するようにしても良い。

【０１４２】

さらに上述の第１～第３の実施の形態においては、ネットワーク５上に設けられ、個人端末（端末装置）２、５１、６０から発信されるコンテンツを監視しながら、当該コンテンツからユーザ識別情報X_{ID}が検出された場合には、当該ユーザ識別情報X_{ID}が個人端末（端末装置）２、５１、６０に割り当てられた固有のユーザ識別情報X_{ID}と一致するか否かに応じて当該個人端末（端末装置）２、５１、６０に所定の通知又は警告を発信する監視サーバ４を構築するようにした場合について述べたが、本発明はこれに限らず、要はネットワーク上にコンテンツを流出したユーザに通知又は警告を与えることができれば、この他種々の構成からなる監視サーバに広く適用することができる。

【０１４３】

さらに上述のように第１の実施の形態においては、配信サーバ３及び端末装置２がネットワーク５を介して接続されたコンテンツ配信システム１において、配信サーバ３では、端末装置２に割り当てられた固有のユーザ識別情報X_{ID}と、

端末装置２側で予め状態が設定された格納定義フラグX_{FLG}とを所定の拡散変調を行うようにして透かし情報X_{WM1}に変換した後、当該透かし情報X_{WM1}をコンテンツに重畳する重畳部１８、拡散変調部１９（重畳手段）と、透かし情報X_{WM1}が重畳されたコンテンツに所定の暗号をかける暗号化部（暗号化手段）１７と、暗号がかけられたコンテンツをネットワーク５を介して端末装置２に送信する送信手段１４とを設け、端末装置２では、コンテンツを受信するネットワークインターフェイス（受信手段）２４と、コンテンツに重畳されている透かし情報X_{WM1}を所定の処理を行うようにしてユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を抽出するＩＤ・フラグ検出部（抽出手段）３４と、ユーザ識別情報X_{ID}の有効性及び又は格納定義フラグX_{FLG}の状態に基づいて、コンテンツにかけられている暗号を解除するデクリプト部（暗号解除手段）３２と、ユーザ識別情報X_{ID}の有効性及び又は格納定義フラグX_{FLG}の状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断するＣＰＵ（判断手段）２０と、判断手段２０の判断結果に応じて、透かし情報X_{WM1}が重畳されているコンテンツを格納するハードディスク装置（格納手段）２３とを有するようにしてコンテンツ配信システム１を構築するようにした場合について述べたが、本発明はこれに限らず、これ以外にも配信サーバ３が個人端末（端末装置）２側で設定したユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を透かし情報X_{WM1}としてコンテンツと共に当該個人端末（端末装置）２に送信することができれば、この他種々の配信サーバ及び端末装置に広く適用することができる。

【０１４４】

またユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}は、拡散変調による透かし情報とするに限らず、そのままフラグ情報として、コンテンツに付加されるようにしてもよい。個人端末（端末装置）側においても、暗号化コンテンツの場合は、セキュリティーが確保されているので、透かし情報を検出せずに、このフラグ情報だけを読むようにしてもよい。

【０１４５】

さらに上述のように第２の実施の形態においては、配信サーバ５２では、個人端末（端末装置）５１に割り当てられた固有のユーザ識別情報X_{ID}及び当該端

末装置側で予め状態が設定された格納定義フラグX_{FLG}をコンテンツに付加する一方、個人端末（端末装置）５１では、受信したコンテンツに付加されているユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を抽出して、当該格納定義フラグX_{FLG}の状態に応じてコンテンツにかけられている暗号を解除し、ユーザ識別情報X_{ID}の有効性に基づいて当該ユーザ識別情報X_{ID}を所定の拡散変調を行うようにして透かし情報X_{WM2}に変換した後、当該透かし情報X_{WM2}をコンテンツに重畳するか否かを判断する。そしてユーザ識別情報X_{ID}の有効性及び又は格納定義フラグX_{FLG}の状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断して、判断結果に応じて透かし情報X_{WM2}が重畳されたコンテンツを格納するようにした場合について述べたが、本発明はこれに限らず、要は個人端末（端末装置）５１においてユーザ識別情報X_{ID}を透かし情報X_{WM2}としてコンテンツにユーザ識別情報X_{ID}を重畳することができれば、この他種々の構成の配信サーバ及び端末装置に広く適用するようにしても良い。

【０１４６】

さらに上述のように第３の実施の形態においては、配信サーバ５２では、個人端末（端末装置）６０に割り当てられた固有のユーザ識別情報X_{ID}及び当該端末装置側で予め状態が設定された格納定義フラグX_{FLG}をコンテンツに付加する一方、個人端末（端末装置）６０では、コンテンツを受信してハードディスク装置（格納手段）２３に格納しておき、当該ハードディスク装置（格納手段）２３から必要に応じてコンテンツを再生した場合、当該コンテンツに付加されているユーザ識別情報X_{ID}及び格納定義フラグX_{FLG}を抽出して、当該格納定義フラグX_{FLG}の状態に応じてコンテンツにかけられている暗号を解除し、ユーザ識別情報X_{ID}を所定の拡散変調を行うようにして透かし情報X_{WM3}に変換した後、当該透かし情報X_{WM3}を暗号が解除されたコンテンツに重畳する。そしてユーザ識別情報X_{ID}の有効性及び又は格納定義フラグX_{FLG}の状態に基づいて、透かし情報X_{WM3}が重畳されたコンテンツをハードディスク装置（格納手段）２３に格納するか否かを判断して、判断結果に応じて透かし情報X_{WM3}が重畳されたコンテンツをハードディスク装置（格納手段）２３に格納するよ

うにした場合について述べたが、本発明はこれに限らず、要は個人端末（端末装置）６０においてユーザ識別情報X_{ID}を透かし情報X_{WM3}としてコンテンツにユーザ識別情報X_{ID}を重畳することができれば、コンテンツをハードディスク装置（格納手段）２３に格納する前後にかかわらず、この他種々の構成の配信サーバ及び端末装置に広く適用するようにしても良い。

【０１４７】

【発明の効果】

上述のように本発明によれば、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信システムにおいて、配信サーバでは、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとを所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報をコンテンツに重畳する重畳手段と、透かし情報が重畳されたコンテンツに所定の暗号をかける暗号化手段と、暗号がかけられたコンテンツをネットワークを介して端末装置に送信する送信手段とを設け、端末装置では、コンテンツを受信する受信手段と、コンテンツに重畳されている透かし情報を所定の処理を行うようにしてユーザ識別情報及び格納定義フラグを抽出する抽出手段と、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、コンテンツにかけられている暗号を解除する暗号解除手段と、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する判断手段と、判断手段の判断結果に応じて、透かし情報が重畳されているコンテンツを格納する格納手段とを設けたことにより、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信システムを実現できる。

【０１４８】

また本発明によれば、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、配信サーバでは、端末装置に割り当てられた

固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとを所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報をコンテンツに重畳する第１のステップと、透かし情報が重畳されたコンテンツに所定の暗号をかける第２のステップと、暗号がかけられたコンテンツをネットワークを介して端末装置に送信する第３のステップとを設け、端末装置では、コンテンツを受信する第４のステップと、コンテンツに重畳されている透かし情報を所定の処理を行うようにしてユーザ識別情報及び格納定義フラグを抽出する第５のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、コンテンツにかけられている暗号を解除する第６のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する第７のステップと、判断結果に応じて、透かし情報が重畳されているコンテンツを格納する第８のステップとを設けたことにより、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信方法を実現できる。

【０１４９】

さらに本発明によれば、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、配信サーバでは、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとをコンテンツに付加する第１のステップと、ユーザ識別情報及び格納定義フラグが付加されたコンテンツに所定の暗号をかける第２のステップと、暗号がかけられたコンテンツをネットワークを介して端末装置に送信する第３のステップとを設け、端末装置では、コンテンツを受信する第４のステップと、コンテンツに付加されているユーザ識別情報及び格納定義フラグを抽出する第５のステップと、格納定義フラグの状態に応じてコンテンツにかけられている暗号を解除する第６のステップと、ユーザ識別情報の有効性に基づいて当該ユーザ識別情報を所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報をコンテ

ンツに重畳するか否かを判断する第７のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する第８のステップと、判断結果に応じて透かし情報が重畳されたコンテンツを格納する第９のステップとを設けたことにより、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信方法を実現できる。

【０１５０】

さらに本発明によれば、配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信方法において、配信サーバでは、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとをコンテンツに付加する第１のステップと、ユーザ識別情報及び格納定義フラグが付加されたコンテンツに所定の暗号をかける第２のステップと、暗号がかけられたコンテンツをネットワークを介して端末装置に送信する第３のステップとを設け、端末装置では、コンテンツを受信して所定の格納手段に格納する第４のステップと、格納手段から必要に応じてコンテンツを再生した場合、当該コンテンツに付加されているユーザ識別情報及び格納定義フラグを抽出する第５のステップと、格納定義フラグの状態に応じてコンテンツにかけられている暗号を解除する第６のステップと、ユーザ識別情報を所定の拡散変調を行うようにして透かし情報に変換した後、当該透かし情報を暗号が解除されたコンテンツに重畳する第７のステップと、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、透かし情報が重畳されたコンテンツを格納手段に格納するか否かを判断する第８のステップと、判断結果に応じて透かし情報が重畳されたコンテンツを格納手段に格納する第９のステップとを設けたことにより、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして

正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信方法を実現できる。

【０１５１】

さらに本発明によれば、コンテンツを管理する端末装置において、コンテンツに、端末装置に割り当てられた固有のユーザ識別情報と、端末装置側で予め状態が設定された格納定義フラグとが所定の拡散変調により変換された透かし情報として重畳されている場合、当該コンテンツに重畳されている透かし情報を所定の処理を行うようにしてユーザ識別情報及び格納定義フラグを抽出する抽出手段と、コンテンツに暗号がかけられている場合、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、当該コンテンツにかけられている暗号を解除する暗号解除手段と、ユーザ識別情報の有効性及び又は格納定義フラグの状態に基づいて、暗号が解除されたコンテンツを格納するか否かを判断する判断手段と、判断手段の判断結果に応じて、透かし情報が重畳されているコンテンツを格納する格納手段とを設けたことにより、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随することとなり、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができ、かくして正規にコンテンツを購入したユーザの不利益を有効に防止し得る端末装置を実現できる。

【図面の簡単な説明】

【図１】

第１の実施の形態によるコンテンツ配信システムの構成を示す略線図である。

【図２】

図１に示す配信サーバの内部構成を示すブロック図である。

【図３】

図１に示す個人端末の内部構成を示すブロック図である。

【図４】

図１に示す監視サーバの内部構成を示すブロック図である。

【図５】

第１の実施の形態によるコンテンツ受信処理手順の説明に供するフローチャー

トである。

【図６】

第２の実施の形態によるコンテンツ配信システムの構成を示す略線図である。

【図７】

図６に示す配信サーバの内部構成を示すブロック図である。

【図８】

図６に示す個人端末の内部構成を示すブロック図である。

【図９】

第２の実施の形態によるコンテンツ受信処理手順の説明に供するフローチャートである。

【図１０】

第３の実施の形態による個人端末の構成を示すブロック図である。

【図１１】

第３の実施の形態によるコンテンツ受信処理手順の説明に供するフローチャートである。

【図１２】

第１～第３の実施の形態による異なるユーザに基づくコンテンツ監視処理手順の説明に供するフローチャートである。

【図１３】

第１～第３の実施の形態によるファイル共有に基づくコンテンツ監視処理手順の説明に供するフローチャートである。

【符号の説明】

１、５０……コンテンツ配信システム、２、５１……個人端末、３、５２……配信サーバ、４……監視サーバ、５……ネットワーク、１０、２０、４０……ＣＰＵ、１３、２３、４３……ハードディスク装置、１８、５６……重畳部、１９、５５……拡散変調部、３４……ＩＤ・フラグ検出部、４６……不正コンテンツ検出部４６、ＲＴ１～ＲＴ３……コンテンツ受信処理手順、ＲＴ４、ＲＴ５……コンテンツ監視処理手順。

【書類名】図面

【図１】

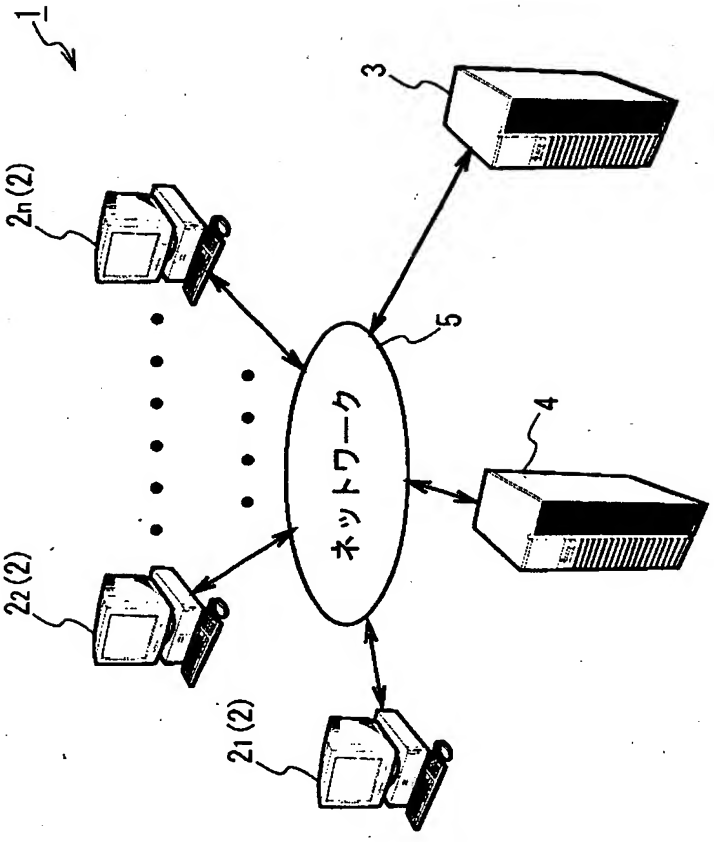

図１　第１の実施の形態によるコンテンツ配信システムの構成

出証特２００３－３０３９２９１

【図２】

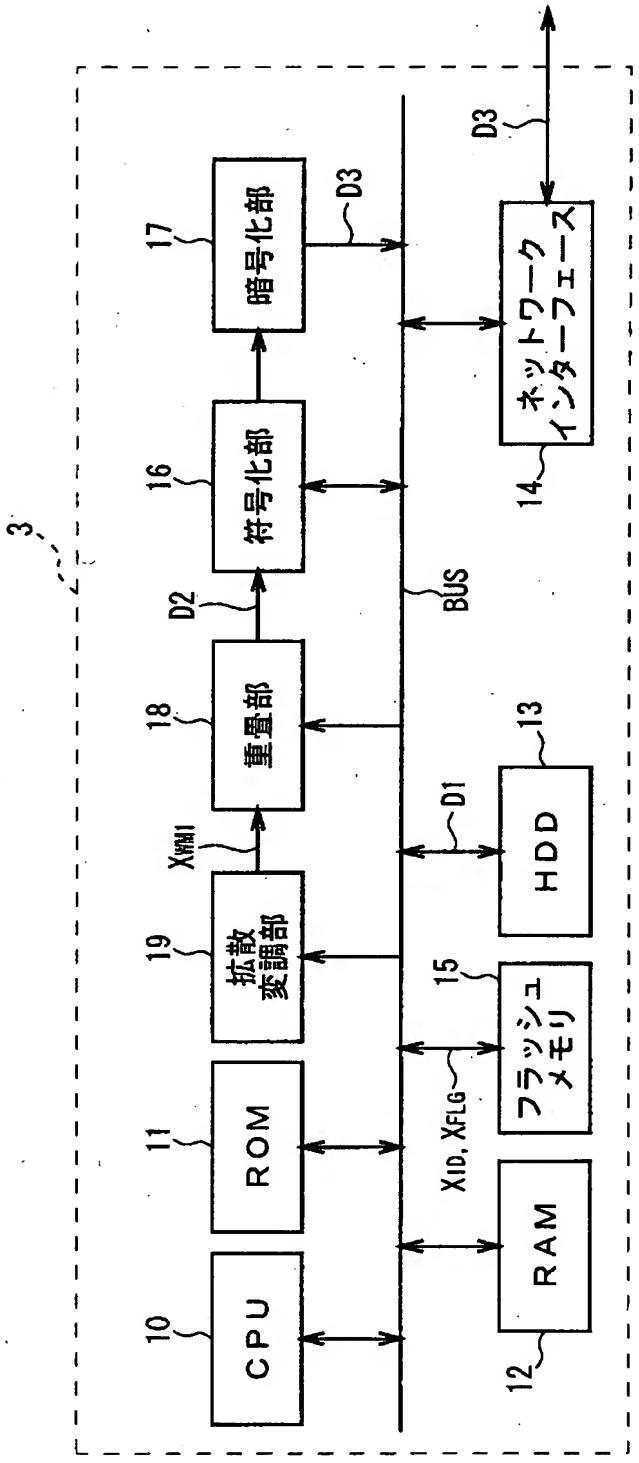

図２　第１の実施の形態による配信サーバの構成

【図３】

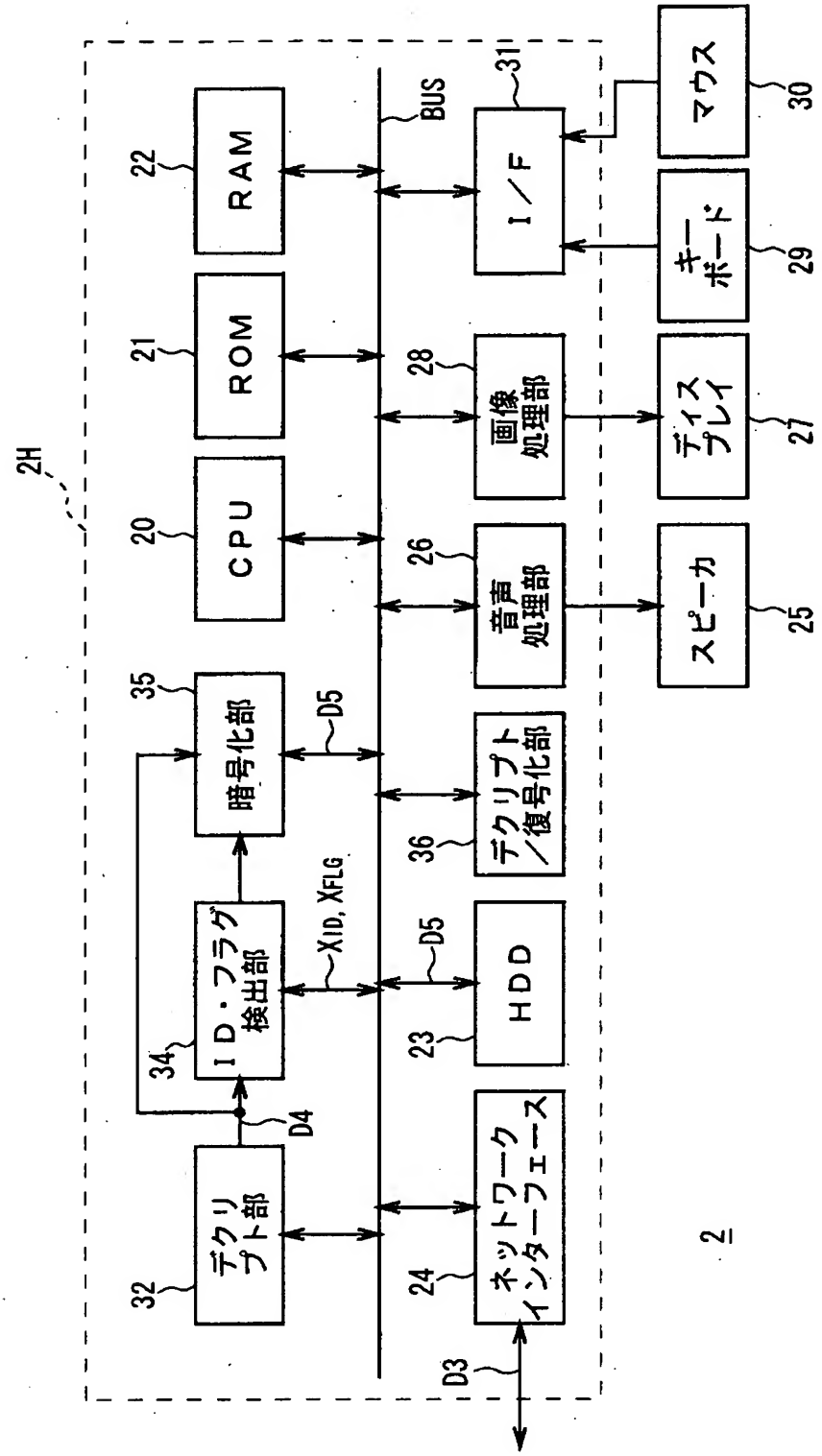

図３　第１の実施の形態による個人端末の構成

【図４】

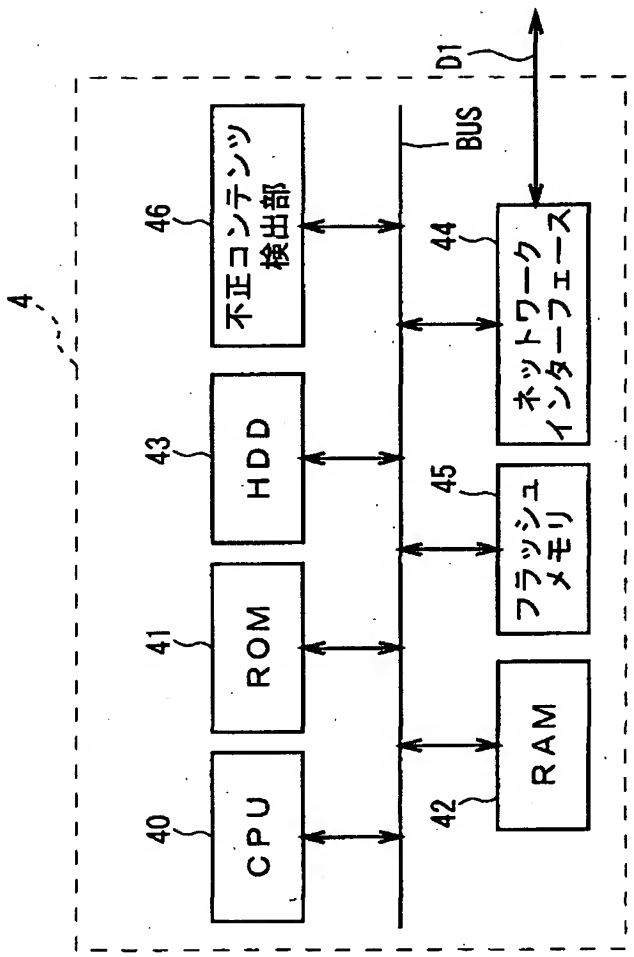

図４　第１の実施の形態による監視サーバの構成

【図５】

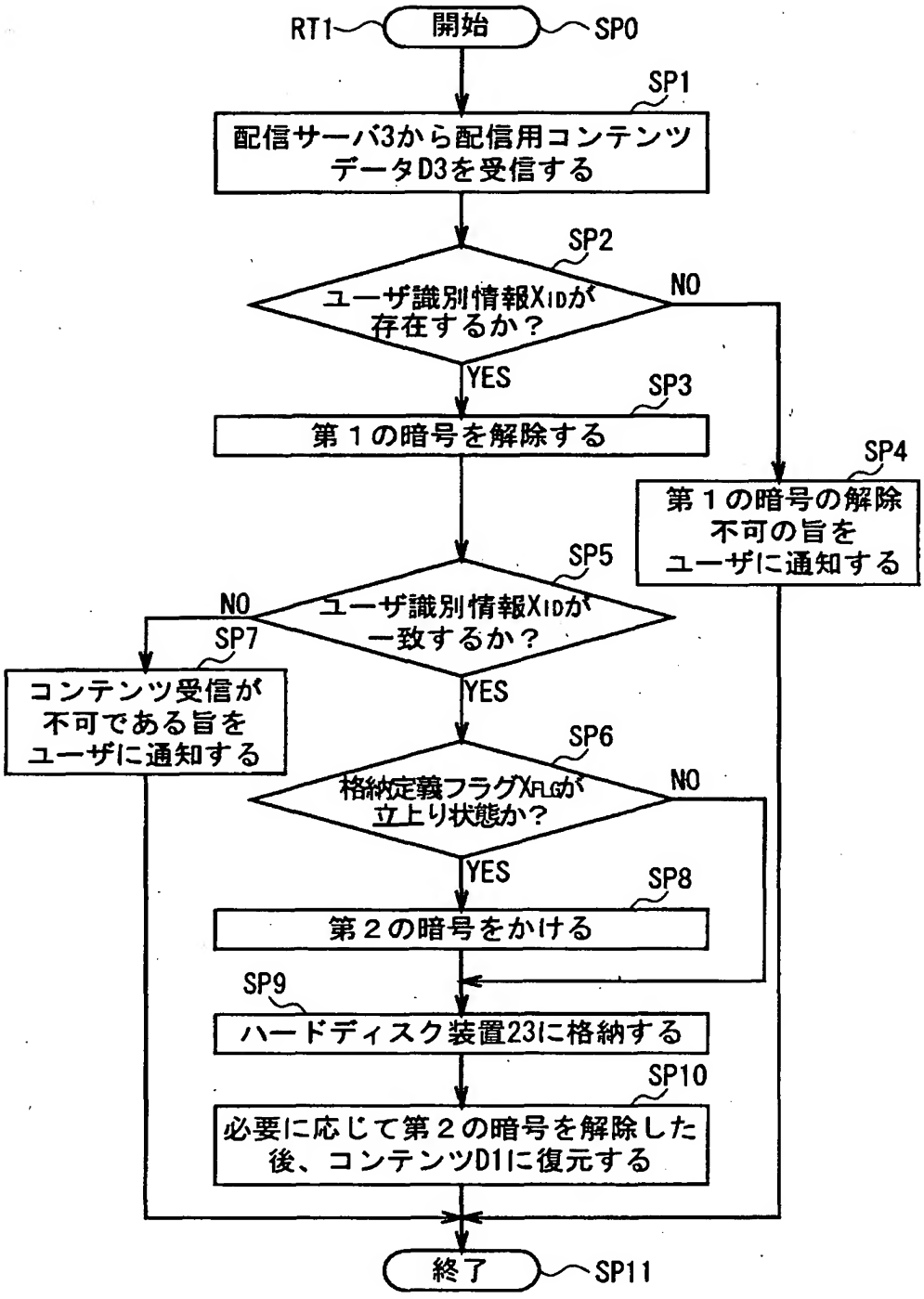

図５　第１の実施の形態によるコンテンツ受信処理手順

【図６】

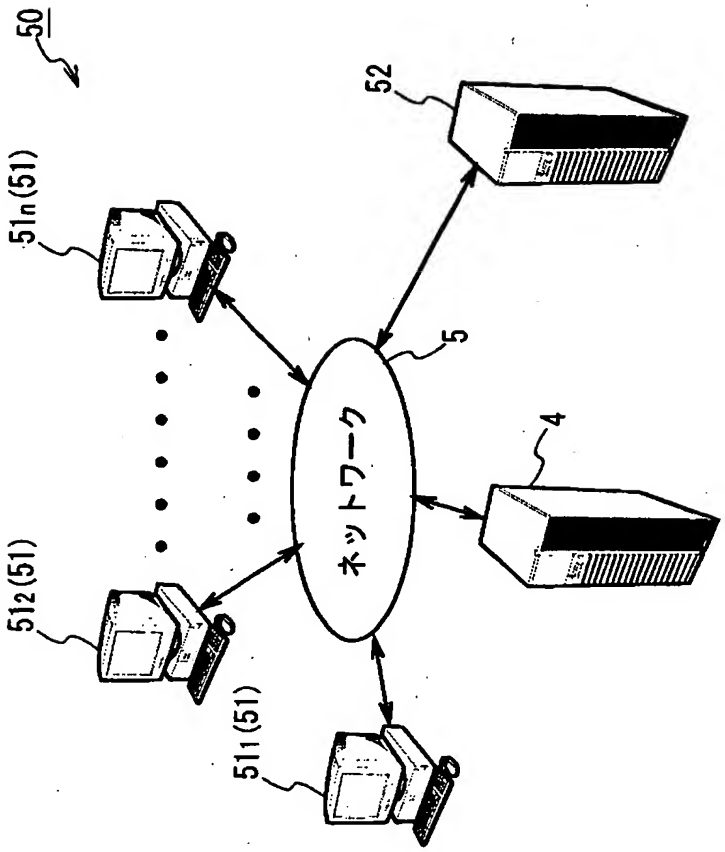

図６　第２の実施の形態によるコンテンツ配信システムの構成

【図７】

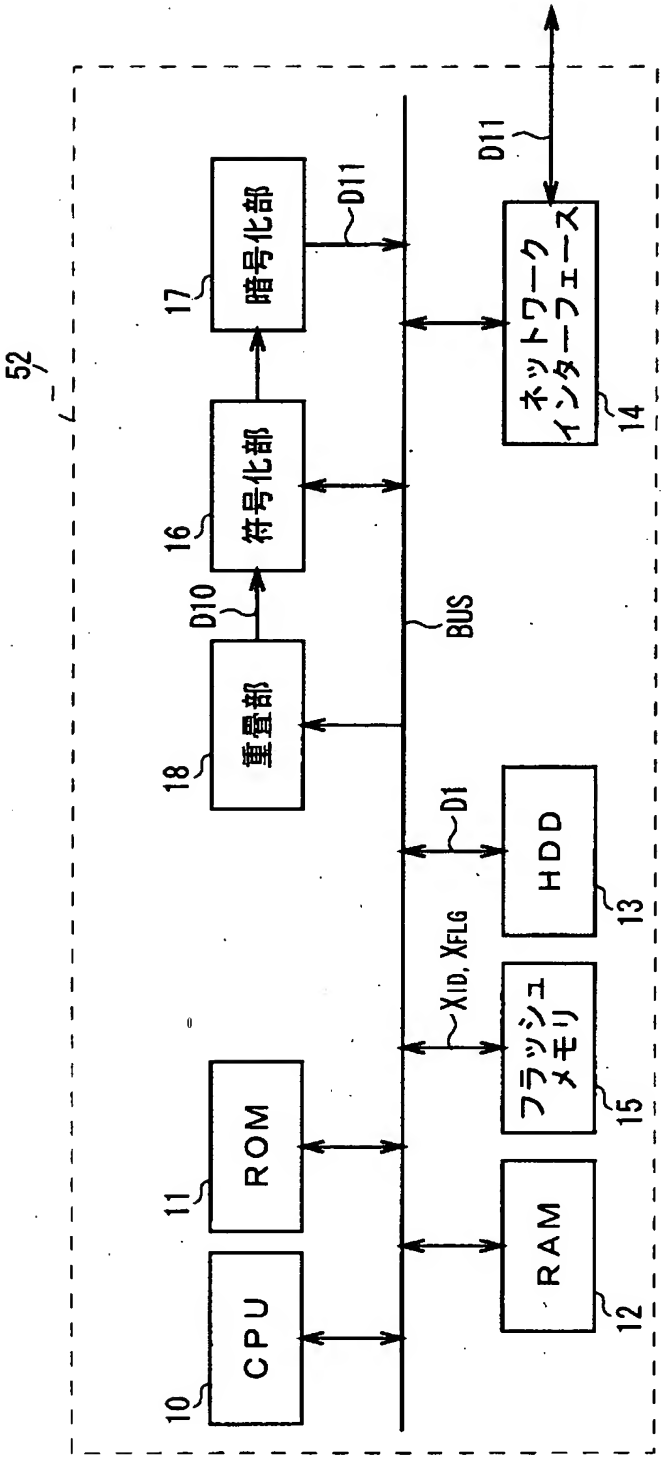

図７　第２の実施の形態による配信サーバの構成

【図８】

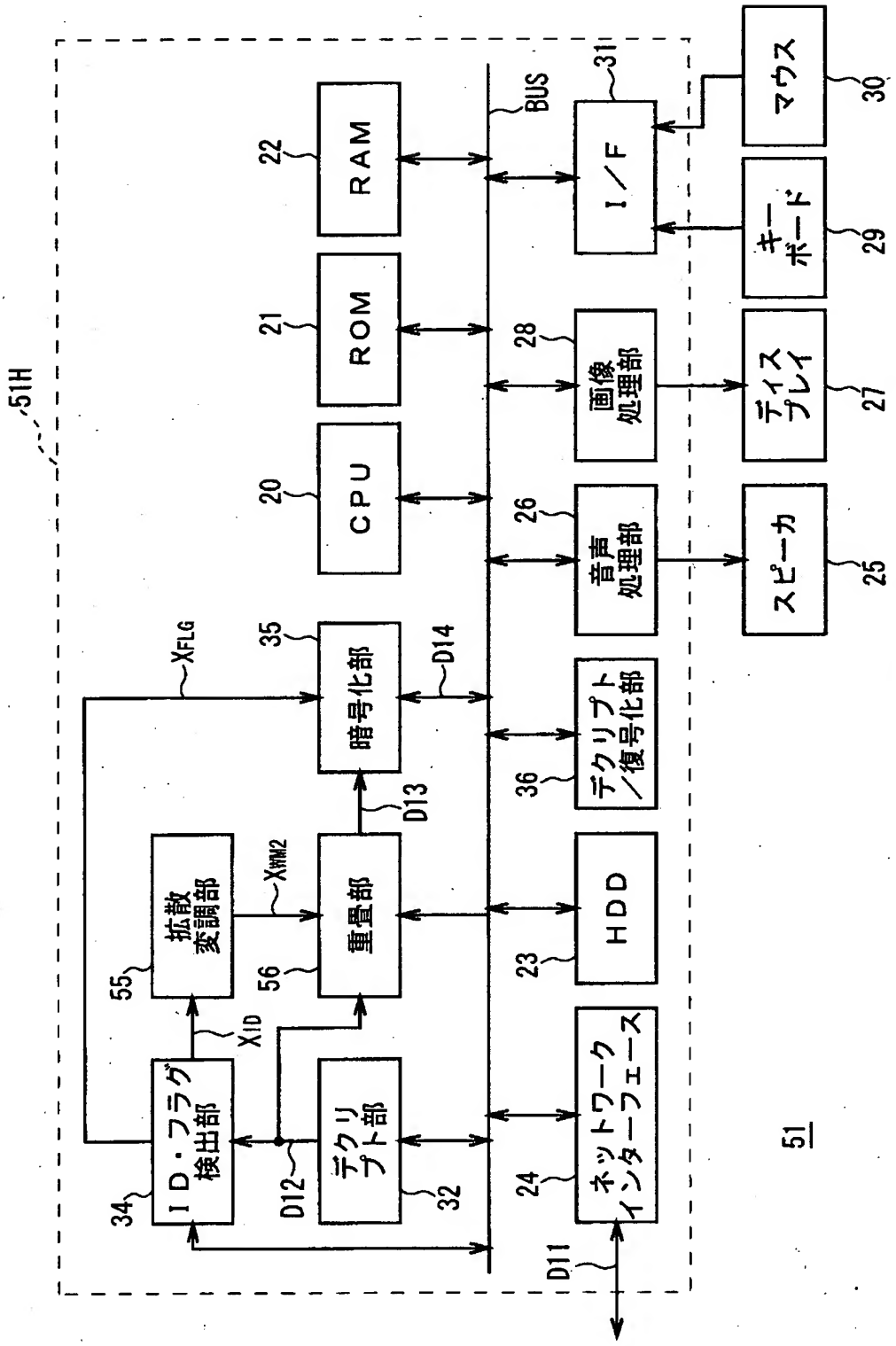

図８　第２の実施の形態による個人端末の構成

【図９】

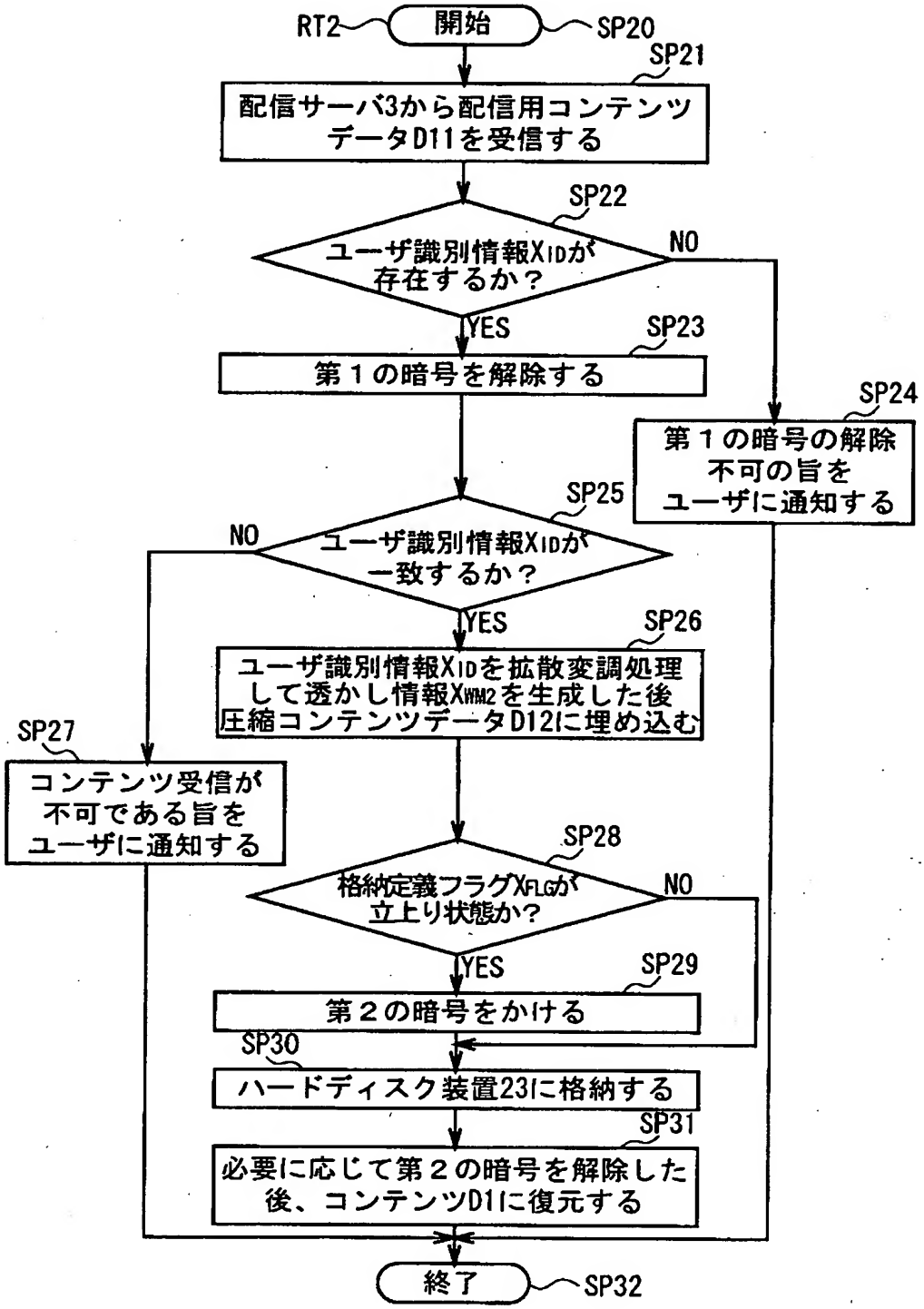

図９　第２の実施の形態によるコンテンツ受信処理手順

【図１０】

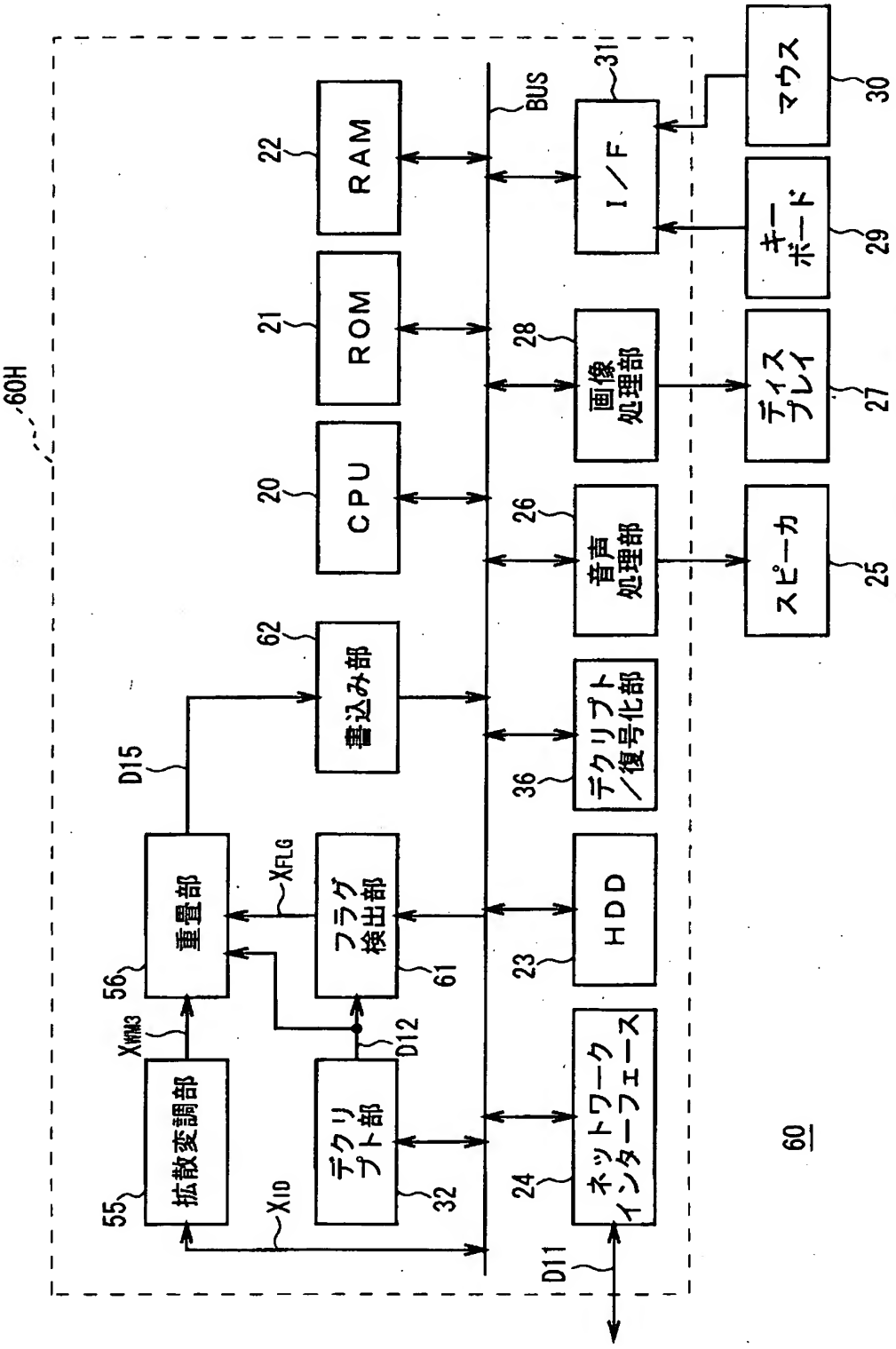

図１０　第３の実施の形態による個人端末の構成

【図１１】

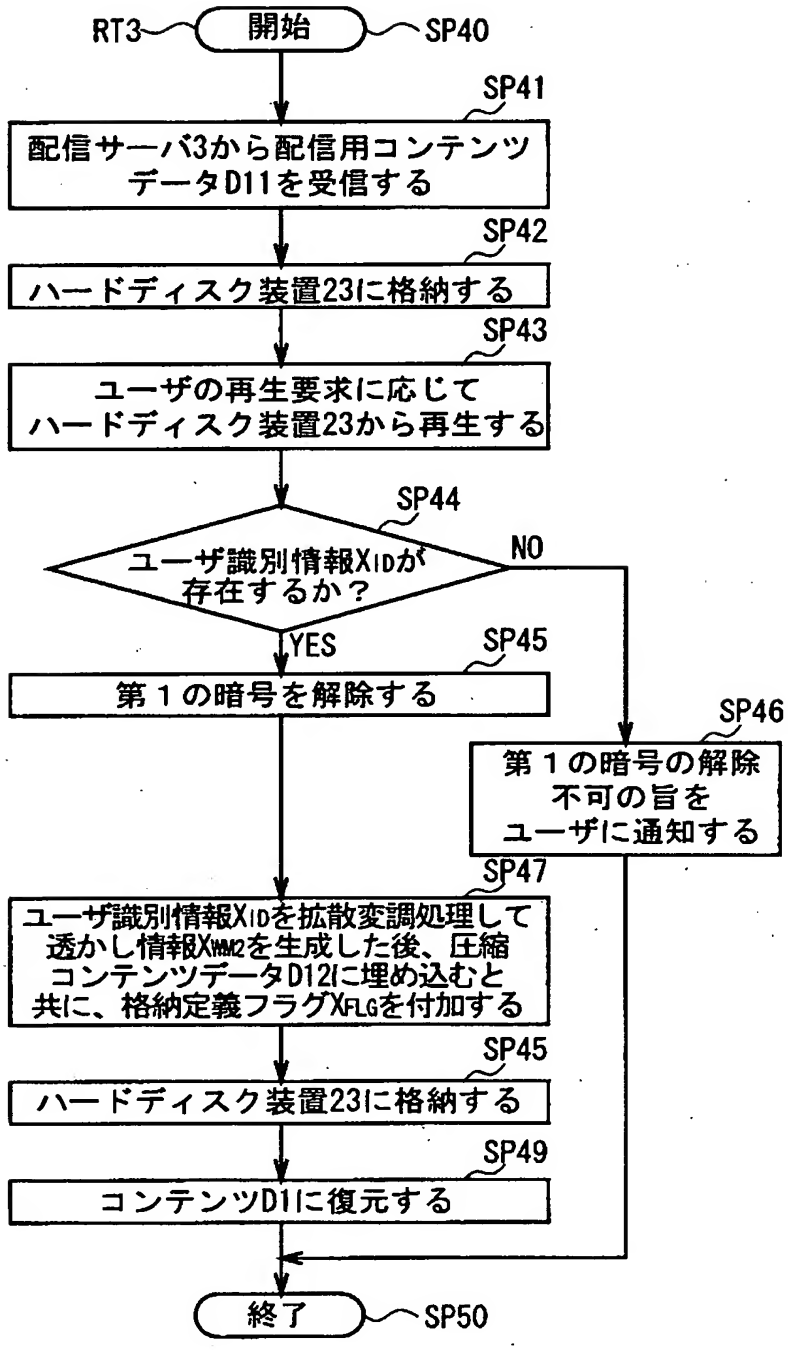

図１１　第３の実施の形態によるコンテンツ受信処理手順

出証特２００３－３０３９２９１

【図１２】

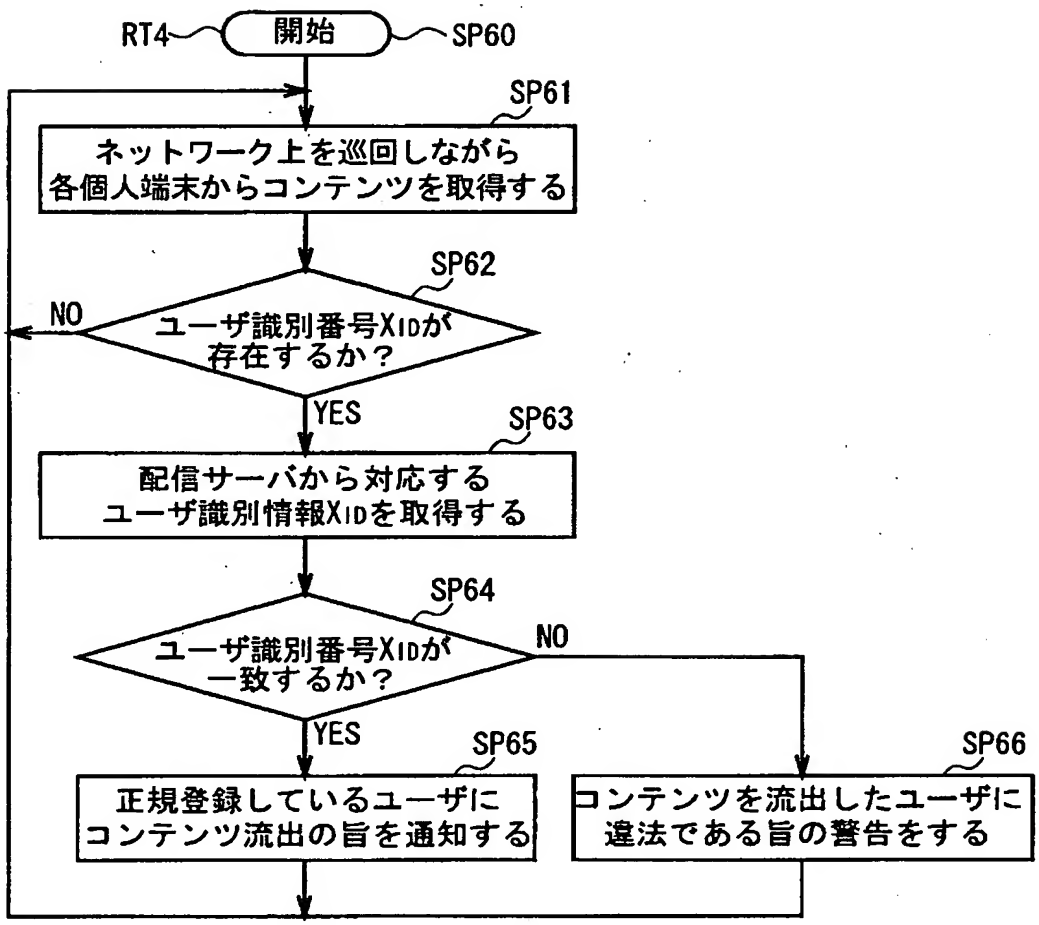

図１２　異なるユーザに基づくコンテンツ監視処理手順

【図１３】

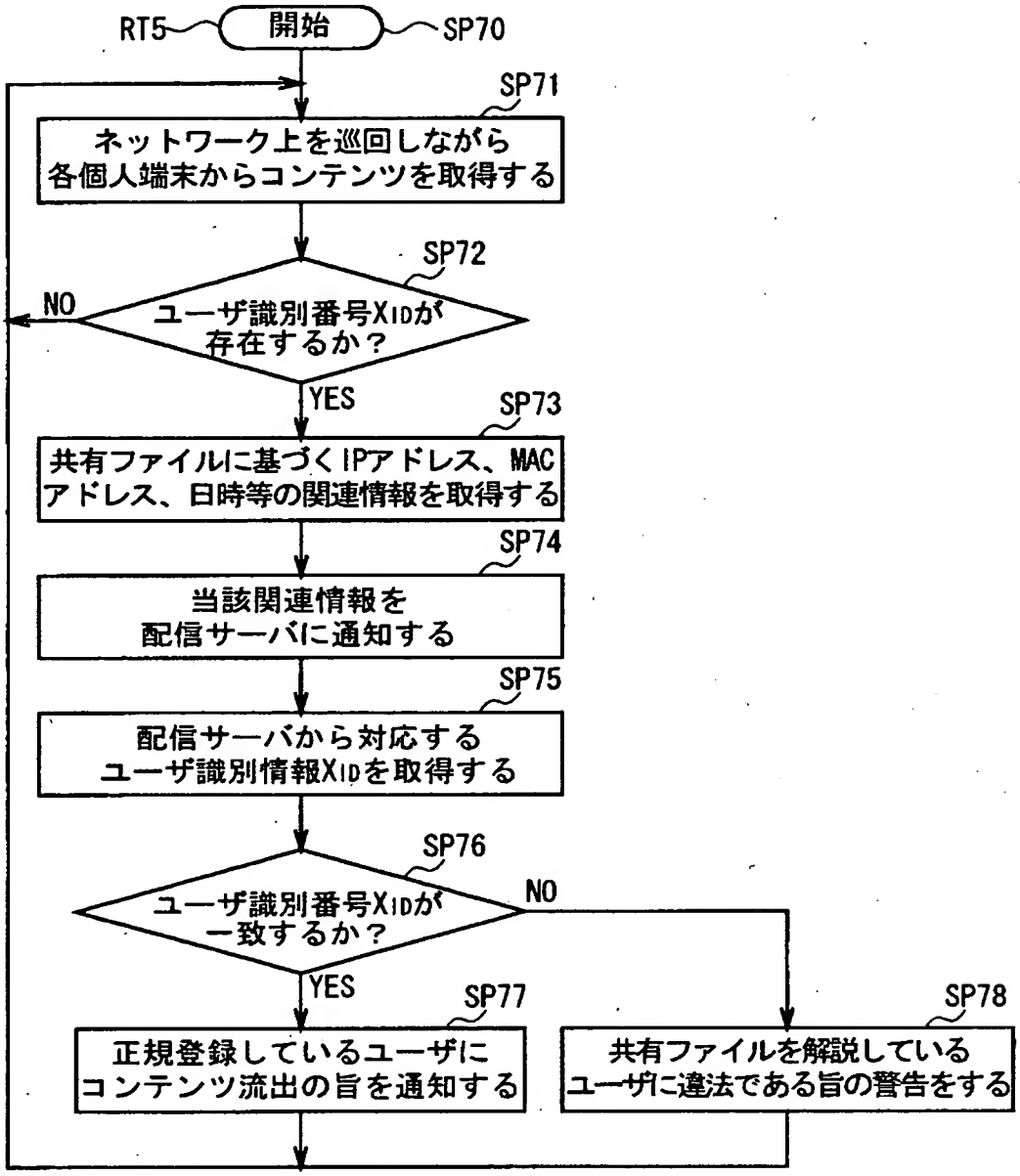

図１３　ファイル共有に基づくコンテンツ監視処理手順

【書類名】　　要約書

【要約】

【課題】

本発明は、正規にコンテンツを購入したユーザの不利益を有効に防止し得るコンテンツ配信システム及びコンテンツ配信方法並びに端末装置を実現しようとするものである。

【解決手段】

配信サーバ及び端末装置がネットワークを介して接続されたコンテンツ配信システムにおいて、端末装置において、後に格納手段からコンテンツが外部に取り出された場合でも、常にユーザ識別情報が付随するようにして、当該コンテンツを有するユーザが不正にネットワーク上に配信しても当該コンテンツの発信元を確実に探索することができるようにした。

【選択図】　　図５

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社